neoware

Neoware Image Manager 4.6
USER MANUAL

neoware

© 2007 by Neoware, Inc.
3200 Horizon Drive,
King of Prussia, PA 19406 USA
Tel.: +1-610-277-8300
Fax: +1-610-771-4200

Email: info@neoware.com

Web: **http://www.neoware.com**

This manual is copyrighted by Neoware, Inc. All rights are reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from Neoware, Inc.

Neoware, Neoware Image Manager, Neoware UbiBoot, Eon, Capio, ThinSTAR, TeemTalk and ezRemote Manager are trademarks or registered trademarks of Neoware, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. MetaFrame, WinFrame, and ICA are registered trademarks of Citrix Systems, Inc. Other trademarks used in this manual are the property of their respective owners.

Disclaimer: The information provided in this manual is intended for instructional purposes only and is subject to change without notice. Neoware, Inc. accepts no responsibility or liability for errors, omissions, or misleading information that may be contained in this manual.

November 2007

Table of Contents

CHAPTER 1 *Introduction 1*

What is Neoware Image Manager? **1**
About This Manual **2**
- Conventions **2**
- Overview of Contents **3**

CHAPTER 2 *Overview of Neoware Image Manager 7*

Software Suite Components **7**
How Neoware Image Manager Works **8**
Neoware Image Manager Boot Process **9**
Adding a New Desktop & Upgrading Hardware **11**
Client Writing Modes **12**
- Normal Mode **12**
- Volatile Mode **12**
- Persistent Mode **13**
- Administrator Mode **13**

High Availability & Fast System Recovery **13**
- Stateless NVD Protocol **13**
- Replacing Servers **13**
- Servers List **14**

Using a Cluster of Servers **14**
Technical Notes **14**
Neoware Image Manager Licenses **15**
Server Licenses **16**
Client Package Licenses **16**
Licenses Explained **16**
Evaluation Version **17**

CHAPTER 3 ***Installing Image Manager Components 19***

System Requirements **19**
Client Requirements **19**
Server Requirements **20**
Network Requirements **22**
Installation Summary **23**
Running the InstallShield Wizard **24**
Image Manager Server Configuration **32**
Disk Storage Required on Server **32**
File Locations on the Server **32**
Uninstalling Neoware Image Manager **35**
Uninstall Procedure **35**
Undoing Client Builder Changes on an HDD-based Configuration **38**

CHAPTER 4 ***Creating a Client Image 39***

Introduction **39**
Using Client Builder **40**
Testing the Image **54**
Advanced Client Builder Options **55**

CHAPTER 5 ***Enabling Clients to Access Images 59***

TFTP & DHCP Server Configuration **59**
Windows **59**
Linux/FreeBSD **60**
Testing the TFTP Service **60**

DHCP Server Configuration **61**
Client Configuration **62**
Troubleshooting **63**

CHAPTER 6 *Assigning Volumes to Clients 65*

Introduction **65**
Running the Image Manager Console **65**
Adding New Clients **67**
Adding a New Group **68**
Assigning a Volume to a Group **69**
Creating or Modifying a Volume **70**
Adding a Volume from Another Configuration File **73**
Changing a Volume's Write Mode **75**
Modifying a Configuration File Currently Running **75**

CHAPTER 7 *Controlling the Use of Images & Volumes 79*

The Image Configuration File **79**
Client Volume Overlay Files **80**
Location of CVol Files **81**
Maximum Size of CVol Files **81**
Volume Write Modes **82**
Admin Mode **83**
CVolwrite Mode **83**
Normal Mode **83**
Volatile Mode **84**
Persistent Mode **84**

CHAPTER 8 *Adding Network Boot Devices to an Image 87*

Overview **87**
Before Using the UbiBoot Extractor & UbiBoot Inserter Tools **89**
Extracting Boot Device Details **90**
Inserting Boot Device Details into an Image **95**
Testing the Image **101**

CHAPTER 9 ***Building a Virtual Hard Disk to Boot any PC or TC 103***

What is Neoware UbiBoot? **103**
Installing Neoware UbiBoot **104**
Potential Incompatibilities **105**
Running Neoware UbiBoot **106**
Using a UbiBoot Enabled Hard Disk **110**
- Learn to Use Unknown Hardware **110**
- Master HD for Building Images **110**
- Detecting New Hardware **111**
- Updating or Removing Drivers for Off-line Devices **112**

Additional Uses for Neoware UbiBoot **113**
- Creating a Windows Installation that can Run Unknown Hardware **113**
- Creating a Windows Installation that can Run Heterogeneous Hardware **113**

HAL Considerations **113**
Mixing ACPI & Non-ACPI Computers **115**
Mixing Unicore & Multicore (or multi-CPUs) Computers **115**
HAL Selection **115**
- Choosing a Specific HAL at Windows Installation **115**
- Downgrading HAL After Windows Installation **116**
- Recommended HAL **117**
- HAL Related Resources **117**

Windows Product Activation **118**
UbiBoot & Microsoft SysPrep **118**
UbiBoot Expiry Date **119**
Troubleshooting **119**

CHAPTER 10 ***Managing Local Hard Disk Access 123***

Introduction **123**
Using the Local HD Manager **123**

CHAPTER 11 ***Windows Product Activation 127***

Introduction **127**
Product Activation Procedure **128**

CHAPTER 12 ***Windows User Profiles 131***

Domain Roaming Profiles **131**
"Local" Roaming Profiles **132**
Folders Redirection **134**

CHAPTER 13 ***Adding Clients & New Software 135***

Adding a New Client **135**
Modifying an HD Image to be Used by Several Clients **136**
- Using Admin Mode **136**
- Using the CVolMerge Tool **137**

Managing & Updating Images Located at Multiple Remote Sites **141**
Restoring a Virtual Volume to an Actual Hard Disk **144**

CHAPTER 14 ***Adding Clients to Windows Domains 147***

Introduction **147**
How the Neoware Domain Wizard Works **147**
Repository for Domain Credentials **148**
- Repository in a Server Directory **148**
- Repository in the System Partition **148**
- Repository in a Non-System Partition **149**

Storing Domain Credentials in an NVDD Server Directory **151**
- Windows XP Professional Clients **151**
- Windows 2000 Professional Clients **159**
- Client Names **159**
- Adding a New Client to the Domain **159**

Storing Domain Credentials on a Non-Volatile Drive **162**
- Client IP Addresses **168**

Adding a New Client to the Domain **168**
Do I Need to Reboot? **169**
Storing Domain Credentials in the System Partition **170**
Client Names **174**
Adding a New Client to the Domain **174**

CHAPTER 15 ***Merging Image & CVol Files 177***
Introduction **177**
Using the CVolCompactor Tool **178**
Using the CVolMerge Tool **178**

CHAPTER 16 ***The Image Manager Console 181***
Introduction **181**
Running the Image Manager Console **181**
The Toolbar **183**
The File Menu **184**
The Edit Menu **184**
The Tools Menu **185**
The View Menu **186**
The Help Menu **186**
Displaying & Changing Properties **186**
Client Properties **187**
Group Properties **191**
Volume Properties **192**
Creating a Volume **193**
The General Tab **193**
The Parameters Tab **195**
The CVol Tab **196**
The Computers tab **197**
The Allowed Computers Tab **198**
Generic Options **199**
The General Tab **199**
The Directories Tab **201**
The Executable Paths Tab **203**

The Network Tab **205**
The Authorized Subnets Tab **206**
The Nvdd Manager **207**
Merging Configuration Files **209**
Password for Remote Administration **210**

CHAPTER 17 ***The NVDD Configuration File 213***
Introduction **213**
The nvdd.smalldisk.vol.conf File **214**
Configuration File Settings **217**
IP Addresses & Port Numbers **217**
Timing **218**
Directory for Client Volumes **218**
Directories for File Transfer **219**
Directory for Binaries **219**
Certificate File **221**
Maximum Size of CVol Files **221**
Computer Name Change Default **222**
Flush Disk Buffers on Write **222**
Number of Processing Units **223**
Buffer Size **223**
User Definitions **223**
Client MAC Address **224**
Computer Name Change **225**
Volume Definitions **225**
Volume ID & Name **225**
Volume Geometry **226**
Volume Type **226**
Volume Integrity **227**
Volume Write Mode **227**
Directory for CVol Files **230**
Cache Size **230**
Allowed Clients **231**
Group Definitions **231**

Client Naming **233**
Setting Client Name using NVD Protocol **233**
Updating Client Name from Client **234**
Enabling Client MultiBoot **235**
Example nvdd.conf with Multi-Volume Support **238**

CHAPTER 18 ***NVDD Server Administration 241***

Introduction **241**
Secured NVDAdmin Protocol **242**
The NVDDAdmin Tool **242**
NVDDAdmin Command Syntax **242**
Command Examples **243**
NVDDAdmin Commands **243**
Considerations Related to File Operations **243**
Considerations Related to put & get Commands **243**
Conventions **244**
Command Descriptions **244**

CHAPTER 19 ***The mPXELdr Configuration File 251***

Introduction **251**
Contents & Syntax **253**
Example mPXELdr .ini File **255**
Keywords **256**
The Include Keyword **256**
The NVDServers Keyword **258**
The BootMode Keyword **260**
The VolSelectionTO Keyword **265**
The PreBootPause Keyword **266**
The ReQueryDHCP-Options Keyword **267**
The NICRxTxQs Keyword **268**

CHAPTER 20 ***Neoware Active Cloner 271***

Introduction **271**

Cloning a Partition **272**
Example Cloning Procedures **273**
Cloning Directly to an Attached Hard Disk **273**
Cloning to a Network Shared Hard Disk **274**
Cloning to Another Image Manager Virtual Hard Disk **275**
Expert Options **276**
Disable Options **276**
Boot Options **277**
Command Line Options **277**
Error Messages **279**
Could Not Copy a File **279**
Client-Specific Settings on the Target System **279**

CHAPTER 21 ***Virtualized Environments 281***

VMWare Environment **281**
Introduction **281**
Streaming Disk Images to Virtual Machines **281**
Provisioning VMs with Image Manager **284**
Running Image Manager Server in a VM **284**
Using Private Networks **284**
Using Public & Private Networks **284**
Performance & Storage Optimization **286**
Image Consolidation **286**
Limitations **286**
Microsoft VirtualPC Virtual Server Environments **287**
Enabling Network Boot **287**
Other Virtualized Environments **288**

APPENDIX A ***Upgrading Image Manager 289***

Important **289**
Upgrading from Previous Versions of Neoware Image Manager 4 **289**
Order of Upgrading Operations **289**

Troubleshooting **291**

APPENDIX B ***The TFTPD Installer 293***

Introduction **293**
Using the TFTPD Installer **294**
Managing the TFTPD Service **295**

APPENDIX C ***Configuring the DHCP Server 297***

Introduction **297**
Before Installing DHCP Server **297**
Configuring the Server **298**
Configuring DHCP **301**
DHCP Reservations **312**
Related Resources **315**

APPENDIX D ***DHCP Reference 317***

How Clients Locate the Image Manager Server **317**
dhcpd.conf File Example **318**
Native DHCP Options **319**
Optional Subkeys & Values **322**
Examples **324**
NetBIOS Name for Clients **326**
Windows DHCP Client **327**

APPENDIX E ***Configuring NVDD as a Windows Service 329***

Introduction **329**
Installation Procedure **329**
Using NVDD as a Service **333**
Configuring NVDD Service Options **333**
Uninstalling the Service **335**
Changing Service Settings **335**

APPENDIX F ***NVDD Reference 337***

Introduction **337**
Command Syntax **337**
- Verbose Mode **337**
- Port Number **338**
- Configuration File **338**
- Log File **338**
- No Lock File Check **338**

APPENDIX G ***NVD.SYS Reference 341***

Introduction **341**
Parameters **341**
- IP Address **341**

APPENDIX H ***File Transfer 345***

Introduction **345**
Root Folder for File Transfers **345**

APPENDIX I ***NVDD Temporary Files 347***

The NVDD Configuration File **347**
The nvdd.conf.LOCK File **348**
USER_REP Files **348**
How to Retrieve Restored Files **349**

APPENDIX J ***Boot Process Comparison 351***

APPENDIX K ***Troubleshooting 355***

Technical Support **355**
Check Versions **355**
PXE **356**
- PXE Implementations **356**
- Etherboot **357**
- PXE Error File Not Found **357**

Issues **357**
Network Adapters **358**
VIA Rhine Family **358**
Servers with Several Network Adapters **359**
Volumes **359**
Multi-Volume Windows 2000 Clients **359**
ACPI **360**
Stand By & Hibernation **360**
Shutdown & Reboot **360**
NVD.SYS Shutdown Delay **360**
Windows 2000 Without the Latest Service Pack **361**
Startup **361**
Clients Using Intel i810 Chipset Under Windows 2000 **361**
Inaccessible Boot Device **361**
Boot Process Stuck **362**
Global Performances **362**
Single Client Running Slowly **362**
Number of Sectors Per Read/Write Request **362**
Network Facilities **363**
Global Connectivity **363**
1000BT/100BT Ethernet Switches **363**
Operations on Virtual Volumes **364**
Delayed Write Failed or Disk Full Error in Client OS **364**
Delayed Write Failed Warnings **365**
Large File Support on Linux 2.2 **368**
Error When Opening a Large Volume **368**
Computer SIDs **368**
Limitations **369**
Data Transfer During Single Client Boot-up **369**
Maximum Clients Attached to a Single Server **369**
Clients Booting Same Images on Several Servers **371**

Maximum Number of Applications Run from an Image **371**
Recommended Network Configuration **372**

APPENDIX L *Copyright Notices & License Terms 375*
Patents **375**
Third Parties Copyrights **375**
Software Copyrighted by Aladdin Enterprises **375**
Software Copyrighted by Paul Kocher **376**
Software Copyrighted by Brian Gladman **376**
Software Copyrighted by Lukas Gebauer **377**
Software Copyrighted by Jordan Russell **379**

Index 381

CHAPTER 1

Introduction

This chapter introduces Neoware Image Manager and describes the scope of this User Manual.

What is Neoware Image Manager?

Neoware Image Manager delivers operating systems and applications on-demand from your server to PCs or thin clients. The server is used as a virtual disk drive, so clients do not require a hard disk or flash memory. All application processing is done by the client.

A single software image containing the operating system, application and hardware drivers for multiple hardware platforms can be streamed on-demand to any PC or thin client - regardless of the device's hardware configuration. PC and thin client users keep their personal configurations and settings, and their data remains unique and secure on the server.

Using Neoware Image Manager you can easily manage multiple images from a graphical interface representing client desktops, groups of desktops and their related hard disk images (volumes). You centrally manage images and define each client's virtual drives in just a few mouse clicks.

- Changes are made to a single image on the server.
- Applications can be deployed instantly.
- Images can be swapped in and out quickly.
- Desktops can be re-purposed just by rebooting.
- Software failure gets repaired by a simple reboot.

You can think of Neoware Image Manager as a network storage product (a SAN product) that makes it possible to boot several clients off a single virtual drive hosted on the server.

About This Manual

This manual describes how to install and use Neoware Image Manager version 4.6. It assumes that you are familiar with Windows and server operating system administration, as well as DHCP/BOOTP and TFTP server configuration.

Conventions

The following names may be abbreviated within the text of this manual:

Neoware Image Manager may be abbreviated to "Image Manager".

Neoware Image Manager Server may be abbreviated to "Image Manager server" or "NVDD server".

Neoware Image Manager Console may be abbreviated to "Image Manager Console" or just "the Console".

Neoware UbiBoot may be abbreviated to "UbiBoot".

Neoware Image Manager Client Builder may be abbreviated to "Client Builder".

Neoware Active Cloner may be abbreviated to "Active Cloner".

The following abbreviations are also used:

"HD" for Hard Disk.

"HDD" for Hard Disk Drive.

"TC" for Thin Client.

Overview of Contents

This manual is divided into the following chapters and appendices:

Chapter 1: Introduction

Introduces Neoware Image Manager and describes the scope of this User Manual.

Chapter 2: Overview of Neoware Image Manager

Provides a brief description of how Neoware Image Manager works.

Chapter 3: Installing Image Manager Components

Describes how to install Neoware Image Manager components on the server and client computers.

Chapter 4: Creating a Client Image

Describes how to use Client Builder to create a client image on the Image Manager server.

Chapter 5: Enabling Clients to Access Images

Describes how to configure the network and clients so that hard disk images can be accessed.

Chapter 6: Assigning Volumes to Clients

Describes how to use the Image Manager Console to assign volumes to clients.

Chapter 7: Controlling the Use of Images & Volumes

Describes the image configuration file settings that determine how clients can use images and volumes.

Chapter 8: Adding Network Boot Devices to an Image

Describes how to add bootable network card details to an image so it can be remote booted on different machines.

Chapter 9: Building a Virtual Hard Disk to Boot Any PC or TC

Describes how to use Neoware UbiBoot to build a virtual hard disk that can boot a range of PC and TC hardware configurations.

Chapter 10: Managing Local Hard Disk Access

Describes how to enable or disable client access to local hard disks.

Chapter 11: Windows Product Activation

Describes how to activate Windows products for Image Manager clients.

Chapter 12: Windows User Profiles

Describes how to configure your Neoware Image Manager system so that clients can use Windows user profiles.

Chapter 13: Adding Clients & New Software

Describes how to add a new client, add new software, and restore a virtual hard disk volume to an actual hard disk.

Chapter 14: Adding Clients to Windows Domains

Describes how to add Neoware Image Manager clients to a Windows domain using the Neoware Domain Wizard.

Chapter 15: Merging Image & CVol Files

Describes how to use the CVolMerge tool to create a new hard disk image from an existing image and a CVol file.

Chapter 16: The Image Manager Console

Describes how to use the Image Manager Console to change settings in an `nvdd` configuration file.

Chapter 17: The NVDD Configuration File

Describes the `nvdd` configuration file and the settings that can be specified in it.

Chapter 18: NVDD Server Administration

Describes the NVDDAdmin tool and NVDAdmin protocol commands for administering a remote NVDD server.

Chapter 19: The mPXELdr Configuration File

Describes the mPXELdr configuration file and the settings that can be specified in it.

Chapter 20: Neoware Active Cloner

Describes how to use Neoware Active Cloner to clone the current system partition to another partition.

Chapter 21: Virtualized Environments

Describes how to use Neoware Image Manager with virtual machines, which can run Image Manager clients or server.

Appendix A: Upgrading Image Manager

Describes how to upgrade from earlier versions of Neoware Image Manager.

Appendix B: The TFTPD Installer

Describes how to use the TFTPD Installer to configure Windows 2000/2003/XP TFTP Server for Image Manager clients.

Appendix C: Configuring the DHCP Server

Describes how to configure the Windows 2000/2003 DHCP server.

Appendix D: DHCP Reference

Describes how clients locate the Neoware Image Manager server, and the DHCP options used.

Appendix E: Configuring NVDD as a Windows Service

Describes how to configure the Image Manager server as a Windows service.

Appendix F: NVDD Reference

Describes the command line options that can be used when launching the `nvdd` server module.

Appendix G: NVD.SYS Reference

Describes the parameters that can be set in the registry entry for the `nvd.sys` driver.

Appendix H: File Transfer

Describes issues relating to the file transfer capabilities of Image Manager.

Appendix I: NVDD Temporary Files

Describes issues relating to temporary files created by the `nvdd` process.

Appendix J: Boot Process Comparison

Provides a side-by-side comparison between a HDD-based boot process and the Neoware Image Manager based boot process.

Appendix K: Troubleshooting

Provides help on how to overcome problems when using Neoware Image Manager with various systems.

Appendix L: Copyright Notices & License Terms

Provides the copyright notices and license terms for software embedded in Neoware Image Manager components.

CHAPTER 2

Overview of Neoware Image Manager

This chapter provides a brief description of how Neoware Image Manager works.

Software Suite Components

Neoware Image Manager consists of the following main components:

- **Neoware Image Manager Server** - Allows the remote boot and central management of Windows 2000, XP, XP Embedded, XP Home, XP Pro desktops (diskless PCs or flashless thin clients) from Windows/Linux/FreeBSD servers.
- **Neoware Image Manager Client Builder** - Enables you to create a virtual disk off an existing hard disk drive.
- **Neoware Image Manager Console** - Allows easy configuration of hard disk drive image servers and allocates configurations and operating modes in a few mouse clicks.
- **Neoware UbiBoot** - Enables a single hard disk drive image to be built that can be used across a wide variety of desktop hardware configurations.
- **Neoware Active Cloner** - A partition duplicator that works on a file by file basis and enables differential cloning and duplication of the current system partition to another partition while Windows is working. The Active Cloner enables very fast back-up operations and allows for optimized image update processes when used with Neoware UbiBoot.

How Neoware Image Manager Works

Neoware Image Manager enables you to quickly build and distribute virtual hard disk images (volumes) to diskless PCs and clients. The procedure is very straightforward and can be summarized as follows.

First of all you would install then run **Neoware Image Manager Server** on a server, then, on another PC (a "client" PC), install and run **Client Builder** on a hard disk containing the required Windows operating system and software configuration. Client Builder will create an image of the hard disk on the server. The hard disk image can be hosted on virtually any type of server, which acts as a virtual hard disk drive. There is no increase in the number of processors required because all application processing is done at the client desktop, not by the server.

Neoware Image Manager client desktops are then configured to use PXE-based remote boot to find the operating system, hardware drivers and applications they need to load from the Image Manager server, instead of loading them from their local hard drive or flash memory. When you turn on the PC or thin client you will immediately receive a complete pre-installed configuration.

The Client Builder will generate a configuration file associated with the hard disk image. This enables you to specify which clients can use the image and how they can use it. The settings in the configuration file can be modified using the **Neoware Image Manager Console**, which provides an easy-to-use graphical user interface.

An example of an Image Manager server setup in a retail organization would be as follows. Each store would have a local Image Manager server providing hard disk images to all the clients in that store. The Head Office would have a server running the Neoware Image Manager Console which would provide central control over the hard disk images being used at each store.

Client desktops can run with different modes of operation, allowing or preventing changes to the desktop by users, while also sharing the same image on the server. For example, in Volatile mode, users will

always boot from the originally defined configuration. User profiles (desktop, shortcuts, favourites, bookmarks, application settings, etc.) may be stored on a remote server and presented according to which user logs into the desktop device. This enables user personalization based on Windows User Profiles while desktops are not dedicated to any one user. However, running desktops in Normal mode allows users to individually configure them, enabling basic per-client product activation and license management.

Neoware Image Manager Boot Process

When it boots, a Neoware Image Manager client performs several steps that are very similar to the HDD boot process. The first steps of the boot process, usually devoted to BIOS and BIOS-based mechanisms, also exist in Neoware Image Manager.

The Network Boot Program named `mPXELdr.BIN` (supplied with Neoware Image Manager), is the first component to be involved in Neoware Image Manager clients boot process. It acts as a BIOS extension and provides a BIOS-based interface for the first step of the boot process (the step that experts call int13h based or “real mode” portion of the boot process).

At first, `mPXELdr.BIN` is downloaded into the client memory using the PXE boot prom capabilities. `mPXELdr.BIN` is then executed. It sets the BIOS extensions (int13h redirector in particular) so that read and write operations of disk drives that are usually BIOS-based can be processed by mPXELdr if the drive is a virtual disk drive. mPXELdr translates these BIOS based disk operations into the corresponding Neoware Virtual Disk (NVD) operations.

NVD is the name of the protocol and technology that enables Neoware Image Manager to share virtual drives with several clients. mPXELdr sends NVD operations as NVD packets, on the Local Area Network, to a server that processes them. The server is a program named nvdd (Neoware Virtual Disk Daemon) that runs on a remote host.

mPXELdr sends an “init” packet to the server to retrieve information about the bootable virtual drives available to the client that runs mPXELdr. If several bootable virtual drives are available, mPXELdr displays a boot menu. The users can then choose the drive to be used as the system (boot) drive.

mPXELdr then loads and runs the MBR (Master Boot Record) of the virtual system drive, just as the BIOS loads and runs the MBR of an actual HDD. The boot process then goes on normally (with all the int13h based read/write operations being handled by mPXELdr and nvdd); MBR locates the active partition, loads and runs the Boot Sector, which loads NTLDR.

NTLDR is Windows 2000/XP/2003 OS loader. It does a lot of things, but in particular, it initializes Windows kernel, then loads and runs the boot device drivers. During a Neoware Image Manager client boot process, NTLDR loads and runs `BDruPD.SYS`, `NVD.SYS` and `DSKIMG.SYS`, which are the Neoware Image Manager core client drivers. These drivers create a pseudo device that Windows considers as a disk drive. The operations on this pseudo device, especially read and write operations, are translated into NVD requests to read or write data on the virtual drive served by nvdd. These requests are processed by nvdd. Windows can then use the Neoware Image Manager virtual system disk drive to finish the loading and execution of the rest of the operating system, just as it does when booted off an actual HDD.

For a comparison between the HDD based boot process and the Neoware Image Manager based boot process, refer to the appendix “Boot Process Comparison” on page 351.

Adding a New Desktop & Upgrading Hardware

Neoware Image Manager provides a set of **UbiBoot** utilities that can enable you to modify a hard disk image so that it is able to serve a range of desktops (PCs and thin clients) with heterogeneous hardware configurations. The UbiBoot utilities are used whenever you want to add a new desktop or upgrade hardware. Note that it is not always possible to create a single image that will be usable with all your hardware and associated features. For example, you cannot create an image that will boot both mono-core and dual-core processor clients that will use the two cores of the dual-core clients.

The administrator has two choices when building an image that can support heterogeneous hardware:

1. Boot the new desktop you want to support on a local device (HDD for instance) using the same OS version as the one in the virtual disk image (e.g. Windows XP Professional with Service Pack 2). Launch **UbiBoot Extractor** on the new desktop. This will create a file that contains "boot details" about the new desktop to support. This file is then given to **UbiBoot Inserter** which is running on a Neoware Image Manager client booted off the disk image you want to modify. UbiBoot Inserter modifies the existing virtual disk image so that it can be used to boot the new desktop type. The new desktop can then be booted off the image and Windows will be able to detect the unknown hardware.

2. Launch **Neoware UbiBoot** on a client actually booted off an Image Manager virtual drive to enhance it (this will enable the operating system on this virtual drive to boot unknown hardware when booted off an actual hard disk drive). Use **Neoware Active Cloner** to transfer the hard disk image to an actual hard disk and make it boot on the new hardware. The hard disk learns to recognize the new hardware configuration, then the administrator only has to rebuild the image on the server using Client Builder. Note that Neoware UbiBoot needs to be launched each time just prior to connecting the hard disk to each new hardware configuration.

Client Writing Modes

Image Manager allows administrators to customize how clients write data to virtual volumes. The main writing modes are described below. Refer to the chapter "Controlling the Use of Images & Volumes" on page 79 for a complete description of all the modes available.

Normal Mode

Normal mode enables a client user to install applications and make system changes without modifying the original hard disk image file. Any changes made by the user are written to a write cache file called a CVol (Client Volume OverLay) file on the server. This enables clients to have different configurations while sharing the same hard disk image file.

This mode saves significant time when administrators want to provide users with a configuration defined on a 'per desktop' basis in a simple way, or when users require complete control of their desktops. Restoring a clean installation for a specific client is just a matter of deleting the write cache file on the server.

Note: *If the common hard disk image file is modified, all per-client customizations will be discarded.*

Volatile Mode

Volatile mode enables clients to use exactly the same volume configuration after every reboot. Anything written to the volume by the client will be lost when rebooted. One of the advantages of this mode is that clients boot up from the server very quickly.

You can use Windows User Profiles (desktop, shortcuts, favourites, bookmarks, application settings, etc.) in Volatile mode. User Profiles are stored on a server and copied to the client volumes at logon time.

Persistent Mode

Persistent mode is similar to Volatile mode except it enables you to retain some customization of the volume for each client, separate from the hard disk image. For example, to retain Windows XP activation data customized for each computer.

Note: *Persistent mode uses the same CVol files as in Normal mode, so if the common hard disk image file is modified, all per-client customizations will be discarded.*

Administrator Mode

Administrator mode is usually reserved for administrators so that they can deploy applications and make system changes to the configuration. All modifications are performed and saved on the actual hard disk image. This mode can also be used for all stations at the same time if each station has its own private volume on the server, making it a very private mode.

High Availability & Fast System Recovery

Stateless NVD Protocol

The NVD (Neoware Virtual Disk) protocol used by the Neoware Image Manager client and server to access virtual drives is completely stateless. This means that even if the network connection fails between the client and the server, operation will resume smoothly as soon as the network connection is re-established.

You can reboot the Image Manager server while clients are still running. Of course, during the time Neoware Image Manager is not running the clients will not be able to access their virtual drives and thus they will not be able to do much. But as soon as the server is up and running, the clients will be able to work again.

Replacing Servers

Neoware Image Manager clients know the server they have to contact by using that server's IP address. This means you can replace a server with another one as long as the new server has the same IP address and the files required by the clients (volume image file and CVol files) are accessible to the new server (if they are stored on Network Storage for instance).

Servers List

Neoware Image Manager clients use an initialization file that the Image Manager boot loader loads and interprets to determine the server to contact from a list of servers. Neoware Image Manager clients can also use a specific DHCP option (DHCP Option 132) to determine the server to contact from a list of servers.

Neoware Image Manager boot loader builds a list of the servers to contact from the initialization file and from DHCP Option 132. If the first server in this list does not answer, the client tries to contact the next server in the list, and so forth. If the client reaches the last server in its list and this server does not answer, it then tries the first server again.

You can use Servers List and license files to achieve a form of load-balancing. A server that has reached the maximum number of clients it can serve will refuse to serve a new client. Then a client that tries to boot off that server will fail and will try the next server. By tuning various different initialization files and/or DHCP options 132 and the license file for each server, you can balance the number of clients that connects to each server in your network.

Using a Cluster of Servers

Using a cluster of servers that are exposed to the outside world as a single IP address is a very good way to add fast recovery and high availability capabilities to the servers.

Technical Notes

- If a network cable is unplugged the session will not crash or 'blue-screen'. The desktop will wait for the network to return.
- If the server fails, the client waits for the server to reboot. No data will be lost as long as the user does not shut down the client and the files on the server (especially CVol files) are free from error loss.
- Neoware Image Manager provides support for various storage options. Hard disk images can be stored on IDE, SCSI, iSCSI, SAN, NAS, RAID, SATA, etc.

- There is no theoretical limitation to the number of clients that can be connected to a single Neoware Image Manager server, as long as there are enough bandwidth and hard disk resources on the network and server to fulfill all the client requests in an acceptable time.
- Neoware Image Manager has little effect on memory or performance requirements of software applications running on the clients. The number of applications that can be run at the same time on the same client depends on the client CPU and available memory.

Neoware Image Manager Licenses

Neoware Image Manager license files are used for the server module to determine how many clients it can serve and the expiration date of the system if any. Each license file also embeds the servers' MAC addresses that are activated so that each license file is usable by only one set of servers.

Please note that you cannot change the server MAC address programmatically (in drivers, NIC EEPROM etc.). If you do so, the Neoware Image Manager system will fail to function properly. You cannot legally use the Neoware Image Manager system with a server where the MAC address has been changed or spoofed (in drivers, NIC EEPROM etc.)

There are two types of license files: Server License and Client Package License. All license files must be located in the same directory where the server module (`nvdd.exe` or `nvdd`) is located. The total number of clients that can be served by a single server is the sum of all the number of clients embedded in the license files.

License files are available when you purchase the Neoware Image Manager system or when you order an evaluation copy.

Server Licenses

A Server License file is required. There can be only one server license file and the server license file must be named `lanpcsrv.lic`. Server license files contain the number of clients and the expiration date(s).

Client Package Licenses

Client Package License files are optional. There can be up to 99 Client Package License files. Client Package License files must be named `lanpcclt`*`NN`*`.lic` (where *`NN`* is a number between 01 and 99). Each Client Package License file contains a number of additional clients.

Note: *You may need to rename the Client Package License files in order for them to comply with the* `lanpcclt`*`NN`*`.lic` *names.*

If you received several Server License files for the same server MAC address, you can rename one of the Server License files to `lanpcclt`*`NN`*`.lic` to make it a Client Package License file. This will allow the server to use the sum of the number of licenses in each Server License file. On the other hand, if you rename the original Client Package License file to `lanpcsrv.lic`, it will not function as a Server License file.

Licenses Explained

Assume that you have three license files:

`lanpcsrv.lic`	is a Server License file for 10 clients.
`lanpcclt01.lic`	is a Clients Package License file for 20 clients.
`lanpcclt04.lic`	is a Clients Package License file for 5 clients.

The server can then serve 10 + 20 + 5 = 35 clients.

Please note that if the Server License file embeds an expiration date, the server will cease to function after this date is reached.

Evaluation Version

If you use an evaluation version of Neoware Image Manager, there are some limitations with the product.

- It is limited to a certain date. The expiration date is displayed in Neoware Image Manager Server logs when the server module starts. The evaluation product cannot be used legally after this date without Neoware's written consent.
- It is limited to a certain maximum number of client computers. The maximum number of clients computers is displayed in Neoware Image Manager Server logs when the server module starts. The evaluation product cannot be used legally with more clients than the maximum number of clients.
- It is limited to the default settings, specifically in terms of network settings and system settings. If available, Neoware technical support (for evaluation versions of the product) is limited to a product using the default settings.

CHAPTER 3

Installing Image Manager Components

This chapter describes how to install Neoware Image Manager components on the server and client computers.

System Requirements

Client Requirements

- PXE 2.x enabled.
- Any CPU supported by the operating system to be downloaded from the Neoware Image Manager server.
- Main memory: 128 MB minimum, 256+ MB recommended.
- Network card (100 Mb/s recommended).

In order to successfully install Neoware Image Manager, you will need at least one client workstation with PXE 2.x capabilities that will be used to create a hard disk or "flash disk" image. This client station must have Windows XP, XPe or Windows 2000 properly installed and configured on a regular hard disk drive, and all the required software applications. It is recommended that the latest service packs, patches, updates and hotfixes are applied to the operating system.

The system partition size (the partition where Windows OS is installed) must be smaller than 2 terabytes. The system partition will be used to build a hard disk image file that will be stored on the Image Manager server. You must be sure that the file system used on the server can handle files the same size as the partition. For instance, if your hard disk image file is created on a FAT32

partition on the server, the partition size cannot be larger than 4 GB because FAT32 does not support files larger than 4 GB. Listed below are the typical maximum file sizes for common file systems.

NTFS File size limited only by size of server volume.

FAT Maximum file size is 2 GB.

FAT 32 Maximum file size is 4 GB.

Ext-2 Maximum file size is 2 GB

Ext-3 Maximum file size is 2 TeraBytes (if LFS support is completely implemented).

UFS 32 GB (with default block size of 8K, default in FreeBSD).

Windows and all the applications must be installed in `C:` drive. The `C:` drive should be the only hard disk partition available to the client workstation. Additional applications can be installed in the free space on the hard disk image after the image has been built. If more storage is required, it is recommended that a network share is used. A network drive (a folder on a Windows or Samba server) may be mounted automatically at boot time. Adding this network drive (and extra applications) can be done after the diskless system has been set up.

The network card should be configured to use Auto Media Detection (in EEPROM and in drivers).

The client BIOS settings must specify that the hard disk is accessed in Automatic mode (or LBA mode if no Automatic mode is available).

Server Requirements

- Operating system: Windows NT/2000/XP/2003, Linux, or FreeBSD (see note below).
- Main memory: 128 MB minimum, 512 MB or more recommended.
- Processor: equivalent to Pentium III 800 or faster.

- Hard drive capacity: 1.5 MB dedicated to Image Manager, plus disk space required to store the client hard disk image files and cache files (the default maximum cache file size is 512 MB per client).

Note: *Some releases of Neoware Image Manager do not include the latest version of Linux/FreeBSD components. If you have such a version and you need Linux/FreeBSD server support, contact your Neoware representative.*

The following server OS have successfully been used to run Neoware Image Manager server:

x86 architecture:

- Windows NT 4, Windows 2000, Windows XP, Windows 2003,
- Suse Linux 9.2,
- Debian Linux (kernel 2.2, 2.4 and 2.6),
- Ubuntu Linux 6.06 (Drapper Drake) and 7.04 (Feisty Fawn),
- RedHat Linux 6.2, 7.1, 7.2, 8.0, 9.0, EL ES 3,
- Mandrake Linux/Mandriva 7.2 and 8.0, 9.0, 10.0, 10.1,
- FreeBSD 4.4 to 6

PowerPC architecture:

- TimeSys Linux

Note: *If your server OS is not listed here, the Linux/FreeBSD version may work as long as you are using a compatible OS and architecture. Other server OS and architecture may be supported on request. If you have such a request, please contact your Neoware representative.*

Neoware Image Manager requires a computer to house the server module. This computer should have a minimum of 128 MB of RAM and must be properly installed and configured. Servers that have to serve a large number of clients should have at least 512 MB of RAM (2GB or more is recommended). It is recommended that the latest

service packs, patches, updates and hotfixes are applied to the server operating system.

A server class Network Adapter is recommended for the Image Manager server network card. You should install the latest NIC (Network Interface Card) drivers for the NICs in the server, which are usually available from the NIC manufacturer web site. These drivers are usually more efficient than the drivers shipped with Windows XP/2000. (On a Windows 2000 server with 3C905C-TX-M, the Neoware Image Manager system is twice as fast with 3Com's NIC drivers than with the NIC drivers shipped with Windows 2000.)

When using multiple clients booting off a single server, a performance bottleneck may occur during network and server hard drive data transfers. It is therefore recommended that you use the fastest hard drives and hard disk controllers available, and to have as much RAM as possible in the server to improve disk caching. Having several hard disk drives in the server can also help increase performance. If there is a RAID adapter in the server, we recommend that you use RAID 1 instead of RAID 5.

Network Requirements

- Ethernet 100 Mb/S or better.
- Ethernet Switching.
- A computer running DHCP service and a computer running TFTP service. (This computer can be the same as the Neoware Image Manager server, another single computer, or two separate computers.)

Switches are preferable to hubs. It is recommended that you enable full duplex communication and flow control. Clients and server must be able to send and receive DHCP packets from and to each other.

TCP/IP connectivity between the server and the clients must be established.

A configurable DHCP (or BOOTP) service must be available on your network. For example, MS-DHCP Server for Windows Server NT/2000/2003, freeware TFTPD32 that includes a DHCP service. If

you are using a Microsoft DHCP server, refer to the appendix "Configuring the DHCP Server" on page 297 for a step-by-step installation procedure.

A configurable TFTP service must be installed and properly configured to serve boot files to PXE PROM. For example, MS-TFTPD for Windows 2000/2003 Server, 3Com freeware tftp server for Windows systems, tftpd daemons shipped with Linux and Unix, freeware TFTPD32. A Samba server can be useful if you use Linux/FreeBSD server. For a Windows TFTPD installation, refer to the appendix "The TFTPD Installer" on page 293.

Installation Summary

The installation procedure consists of two stages. First you need to run the Neoware Image Manager InstallShield Wizard on the server and then again on the client to install the relevant software components. Secondly (optionally), you need to configure the server by copying various files into the directory that will contain the hard disk images (if the default location does not suit your requirements - due to not enough available storage space for example).

The server will host the NVDD (Neoware Virtual Disk Daemon) server module and, eventually, the hard disk images that clients will access. This server must be on the same LAN as the clients that will access the images, and must be running either Windows NT/2000/XP/2003 or Linux/FreeBSD. The Neoware Image Manager Console, which enables you to control how images are assigned and used by clients, can either be installed on the NVDD server (if it runs Windows OS) or on a remote PC running Windows OS.

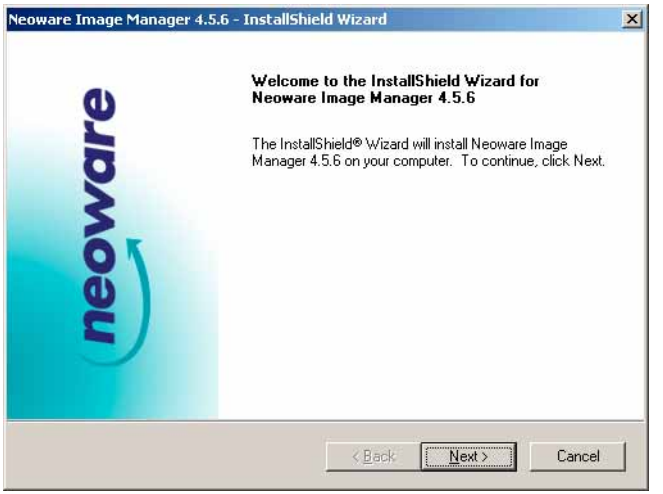
The client computer will provide the basis for the hard disk image that will eventually be created. The InstallShield Wizard will install various tools to enable you to build an image that can be served to clients from the NVDD server.

Running the InstallShield Wizard

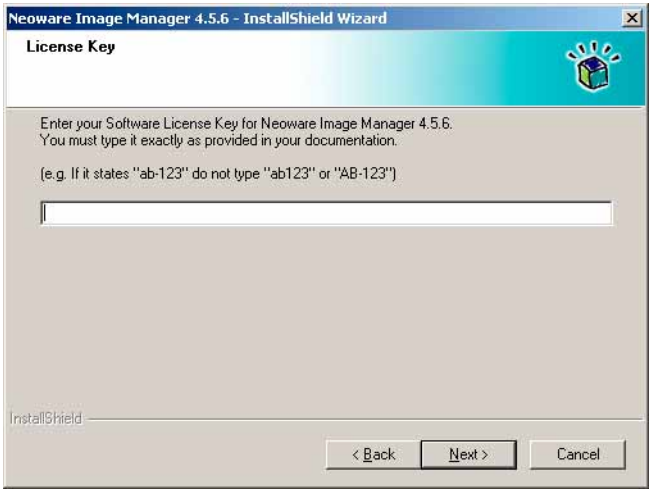
You will need to run the InstallShield Wizard on the server (or a Windows PC if the server is running Linux or FreeBSD - see note below) and then again on the client computer to install the relevant Neoware Image Manager software components.

Note: *If you want to install Neoware Image Manager on a server running Linux or FreeBSD, you will need to run the InstallShield Wizard on a Windows PC, selecting* ***Decompress*** *as the* ***Setup type****, then copy the server software component files installed on the Windows PC to the server.*

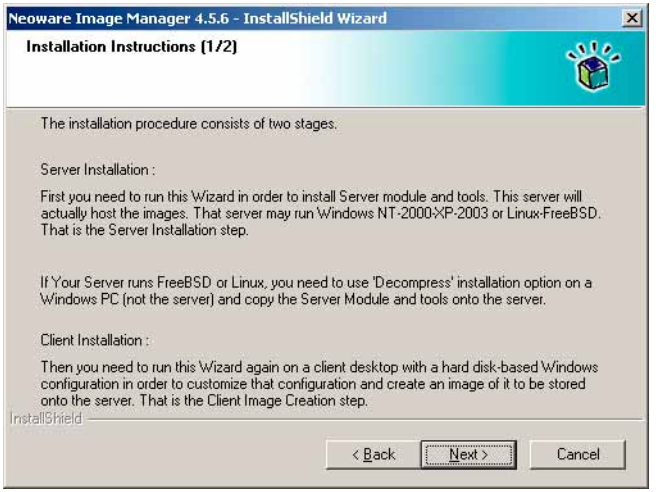
1 Run the Neoware Image Manager InstallShield Wizard by inserting the Neoware Image Manager disk into your CD drive, or by starting the install using the download from Neoware.com.


Neoware Image Manager 4.5.6 - InstallShield Wizard
neoware
Welcome to the InstallShield Wizard for Neoware Image Manager 4.5.6
The InstallShield® Wizard will install Neoware Image Manager 4.5.6 on your computer. To continue, click Next.
< Back
Next >
Cancel

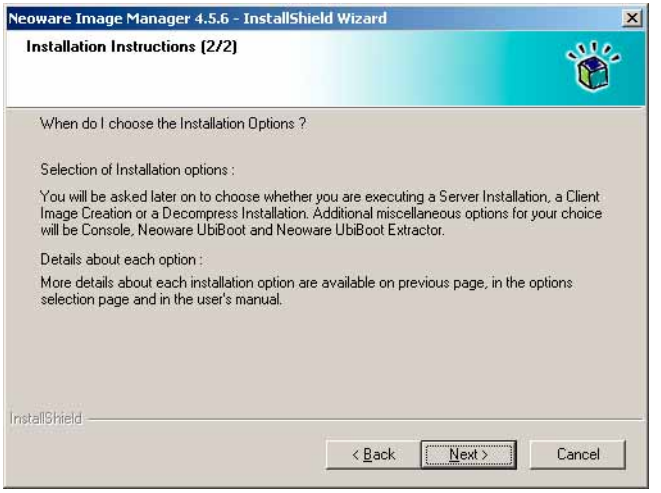
2 Click **Next** to begin the install process.


Neoware Image Manager 4.5.6 - InstallShield Wizard
License Key
Enter your Software License Key for Neoware Image Manager 4.5.6.
You must type it exactly as provided in your documentation.
(e.g. If it states "ab-123" do not type "ab123" or "AB-123")
InstallShield
< Back
Next >
Cancel

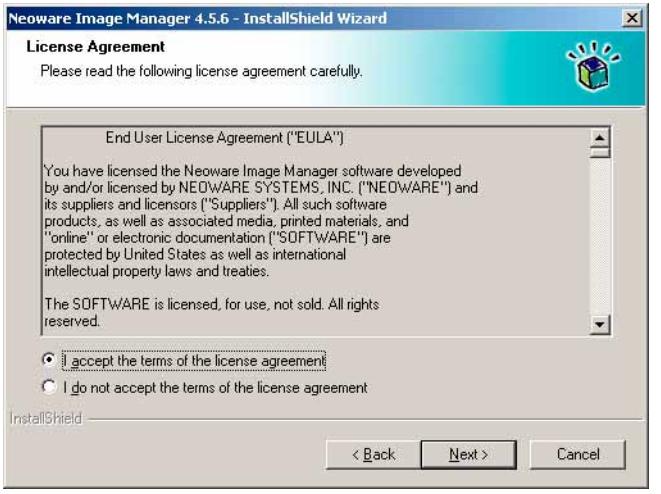
3 Type in your software **License Key** exactly as provided in your documentation, then click **Next**.


Neoware Image Manager 4.5.6 - InstallShield Wizard
Installation Instructions (1/2)
The installation procedure consists of two stages.
Server Installation :
First you need to run this Wizard in order to install Server module and tools. This server will actually host the images. That server may run Windows NT-2000-XP-2003 or Linux-FreeBSD. That is the Server Installation step.
If Your Server runs FreeBSD or Linux, you need to use 'Decompress' installation option on a Windows PC (not the server) and copy the Server Module and tools onto the server.
Client Installation :
Then you need to run this Wizard again on a client desktop with a hard disk-based Windows configuration in order to customize that configuration and create an image of it to be stored onto the server. That is the Client Image Creation step.
InstallShield
< Back
Next >
Cancel

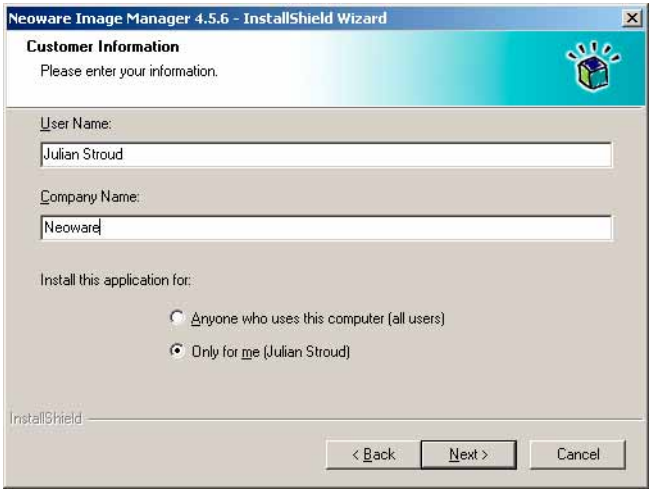
4 This and the following dialog provide instructions on how to install the software. Click **Next** to continue.


Neoware Image Manager 4.5.6 - InstallShield Wizard
Installation Instructions (2/2)
When do I choose the Installation Options ?
Selection of Installation options :
You will be asked later on to choose whether you are executing a Server Installation, a Client Image Creation or a Decompress Installation. Additional miscellaneous options for your choice will be Console, Neoware UbiBoot and Neoware UbiBoot Extractor.
Details about each option :
More details about each installation option are available on previous page, in the options selection page and in the user's manual.
InstallShield
< Back
Next >
Cancel

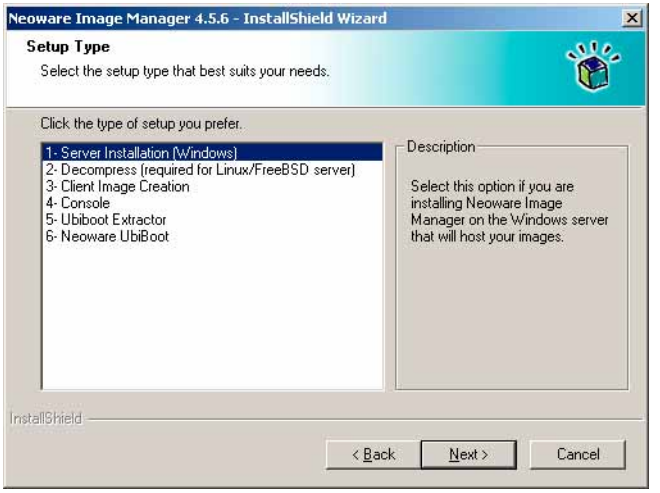
5 Click **Next** to continue.


Neoware Image Manager 4.5.6 - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
End User License Agreement ("EULA")
You have licensed the Neoware Image Manager software developed by and/or licensed by NEOWARE SYSTEMS, INC. ("NEOWARE") and its suppliers and licensors ("Suppliers"). All such software products, as well as associated media, printed materials, and "online" or electronic documentation ("SOFTWARE") are protected by United States as well as international intellectual property laws and treaties.
The SOFTWARE is licensed, for use, not sold. All rights reserved.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
InstallShield
< Back
Next >
Cancel

6 Read the License Agreement and, if you agree to the terms, select the **I accept** option then click **Next**.



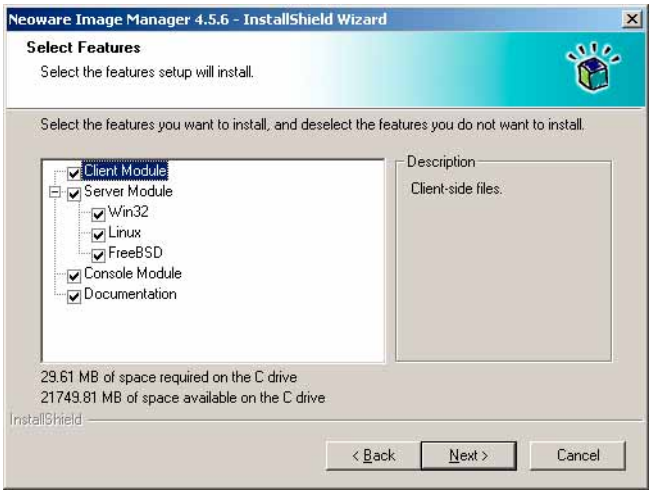
7 Enter the **User Name** and **Company Name** and specify if the application is to be installed for a single user or multiple users. It is usually recommended to install only for you (the administrator) so that users do not have easy access to Neoware Image Manager components that are usually reserved for administrators. Click **Next** to continue.


Neoware Image Manager 4.5.6 - InstallShield Wizard
Setup Type
Select the setup type that best suits your needs.
Click the type of setup you prefer.
1- Server Installation (Windows)
2- Decompress (required for Linux/FreeBSD server)
3- Client Image Creation
4- Console
5- Ubiboot Extractor
6- Neoware UbiBoot
Description
Select this option if you are installing Neoware Image Manager on the Windows server that will host your images.
InstallShield
< Back
Next >
Cancel

8 Select the type of installation required from the following options:

Server Installation (Windows)
Select this option if you are installing Neoware Image Manager on the Windows server that will host your images.

Decompress (required for Linux/FreeBSD server)
Select this option if you plan to run Neoware Image Manager server on a Linux/FreeBSD server that will host your images (you will need to install onto a Windows PC then copy the Server Module and tools onto your server), or in order to perform a simple decompression without shortcuts creation in the **Start** menu. This Wizard will decompress the components of the distribution archive (selected in the next dialog - shown below) into a folder tree.



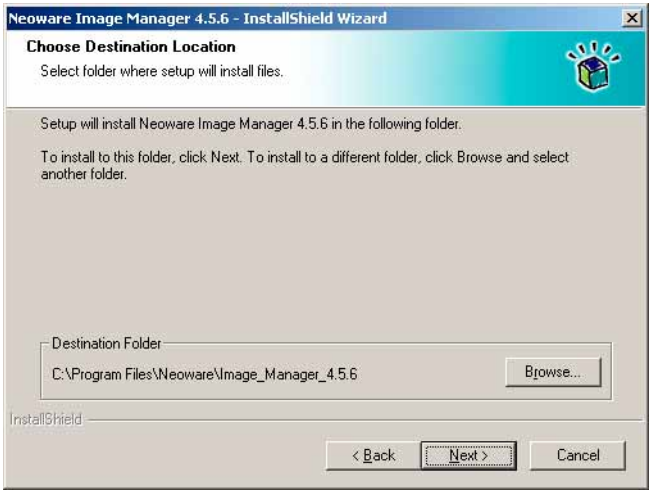
Client Image Creation
Select this option if you are running this InstallShield Wizard on a client desktop. This will install the components that you will run to customize the Windows-based configuration on that desktop's hard disk, and to create an image of it for storing on the server.

Console
Select this option if you would like to install only the Neoware Image Manager Console on a computer running a Windows OS.

UbiBoot Extractor
Select this option if you are installing UbiBoot Extractor on a client machine that needs to be added to the current capabilities of existing images.

Neoware UbiBoot
Select this option if you are installing Neoware UbiBoot on a client machine in order to enhance an existing Virtual Disk Drive so that it will support new hardware platforms.

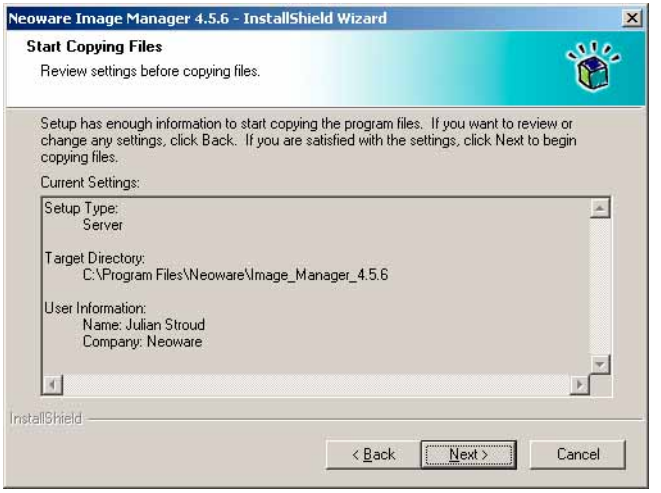
9 Click **Next** to continue. (Note that if **Decompress** was selected, an additional dialog will be displayed before the one shown below, allowing you to select the features you want to install.)


Neoware Image Manager 4.5.6 - InstallShield Wizard
Choose Destination Location
Select folder where setup will install files.
Setup will install Neoware Image Manager 4.5.6 in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\Neoware\Image_Manager_4.5.6
Browse...
InstallShield
< Back
Next >
Cancel

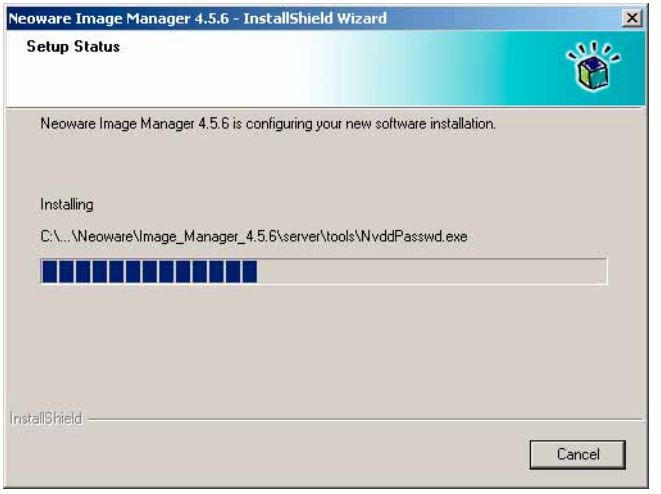
10 Specify the directory where the software components will be installed. The default directory is:

`C:\Program Files\Neoware\Image_Manager_4.6`

11 Click **Next** to review the settings before continuing.


Neoware Image Manager 4.5.6 - InstallShield Wizard
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Setup Type:
Server
Target Directory:
C:\Program Files\Neoware\Image_Manager_4.5.6
User Information:
Name: Julian Stroud
Company: Neoware
InstallShield
< Back
Next >
Cancel

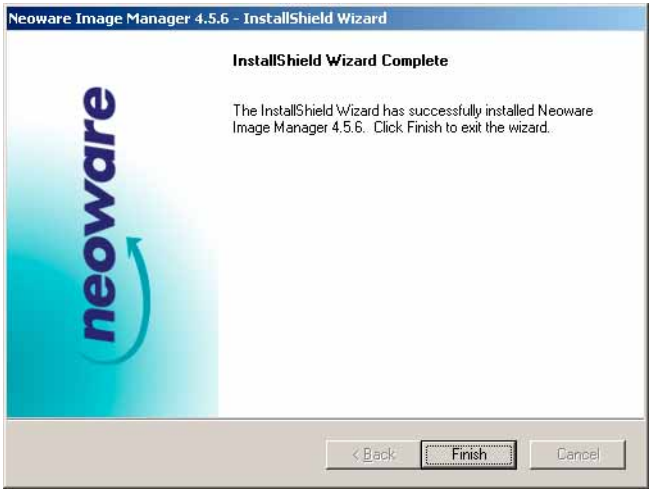
12 If the settings are correct, click **Next** to begin installing the files to the specified location. A progress bar will indicate the current status of the installation.



Note that if the destination device does not have enough disk space for the software to be installed, the following message will be displayed:

Feature transfer error
Feature: Client Installation
Component: Documentation_Files
File: C:\Program Files\Neoware\NIM\Neoware Image Manager 4.5.2\docs\LANP4a97.rra
Error: There is not enough space on the disk.
OK

13 When the installation has been completed, click **Finish**.


Neoware Image Manager 4.5.6 - InstallShield Wizard
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed Neoware Image Manager 4.5.6. Click Finish to exit the wizard.
neoware
< Back
Finish
Cancel

14 Now that the software components have been installed, you need to configure the server as described in the section "Image Manager Server Configuration" on page 32.

If you want to remove the Neoware Image Manager software from your computer, refer to the section "Uninstalling Neoware Image Manager" on page 35.

Image Manager Server Configuration

Disk Storage Required on Server

The Image Manager server must have a partition containing enough free space to contain all the virtual hard disks required by clients. A virtual hard disk consists of a hard disk image file plus a CVol (Client Volume OverLay) write cache file that will contain all data written by the clients. The contents of the CVol files can be retained or deleted when the clients reboot. The hard disk image will be the size of the client partition from which the image was created.

The amount of disk storage needed on the Image Manager server for virtual hard disks is dependent on the mode of operation.

If the clients are using a shared image in Volatile mode, Windows XP Pro and Office 2000 can utilize less than 2 GB. Let us assume that the image size is 2 GB. Every CVol file would use 512 MB maximum and they are deleted at each reboot.

If the user is using their own unique virtual hard disk image in Normal mode, then the CVol files will grow in size. As the Windows file system works so that every sector will be written on eventually, the worst case would be 2 GB for the hard disk image and 2 GB per client. If every sector was rewritten, the CVol files could take up to the virtual hard disk image size. The average case would be when the virtual HD image is updated regularly (once per quarter). This would be approximately 2 GB for the HD and 800 MB per client. Some Windows settings, such as virtual memory settings, have an impact on the size of CVol files.

File Locations on the Server

The following procedure assumes you have already installed the **Server** components of the Neoware Image Manager using the InstallShield Wizard described earlier.

1. Navigate to the directory on the server containing the installed Neoware Image Manager software.

   If you performed a **Server** or **Server with Console** installation, the default directory is:

```
C:\Program Files\Neoware\Image_Manager_4.6
```

If your server runs Linux or FreeBSD OS, the required server module and server tools are stored in the following subdirectory of the target directory in which the Neoware Image Manager archive was decompressed:

```
Server\Linux or Server\FreeBSD
```

Server or **Server with Console** installation: Only Windows versions of the server module (`NVDD.EXE`) and server tools are copied to the following default directory:

```
C:\Program Files\Neoware\Image_Manager_4.6\Server
```

Decompress installation: In the `Server` directory you will find three subdirectories labelled `FreeBSD`, `Linux` and `Windows`, which contain versions of the NVDD server module, one for Windows NT/2000/XP/2003, two for Linux (one statically linked to libraries, the other will dynamically load the required libraries), and two for FreeBSD (static and dynamic, as for Linux):

`NVDD.EXE` is for Windows NT/2000/XP/2003

`nvdd` is for Linux/FreeBSD

2. If required, copy the relevant NVDD file for the operating system you are using into a directory in the server partition where the virtual hard disks will be stored.

3. If required, copy the files `SmallDisk.vol` and `nvdd.smalldisk.vol.conf` from the `Server` directory to the directory containing the NVDD server module.

4. Copy the server license file to the directory containing the NVDD server module. Optionally copy the clients package license files to the same directory.

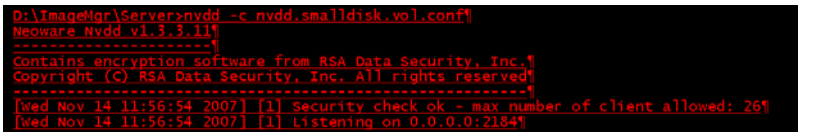
   ***Note**: The license file will be sent to you (if you are evaluating Image Manager), or generated by you from our dedicated web pages (**http://license.neoware.com**) if you purchased the product.*

This completes the Neoware Image Manager server initial configuration. You can test that the NVDD server module is installed correctly by navigating to the directory containing NVDD then typing one of the following at the command prompt to launch it:

Windows system: `nvdd -c nvdd.smalldisk.vol.conf`

Linux/FreeBSD system: `./nvdd -c nvdd.smalldisk.vol.conf`

You should see various messages similar to that shown in the illustration below.


D:\ImageMgr\Server>nvdd -c nvdd.smalldisk.vol.conf
Neoware Nvdd v1.3.3.11
Contains encryption software from RSA Data Security, Inc.
Copyright (C) RSA Data Security, Inc. All rights reserved
[Wed Nov 14 11:56:54 2007] [1] Security check ok - max number of client allowed: 26
[Wed Nov 14 11:56:54 2007] [1] Listening on 0.0.0.0:2184

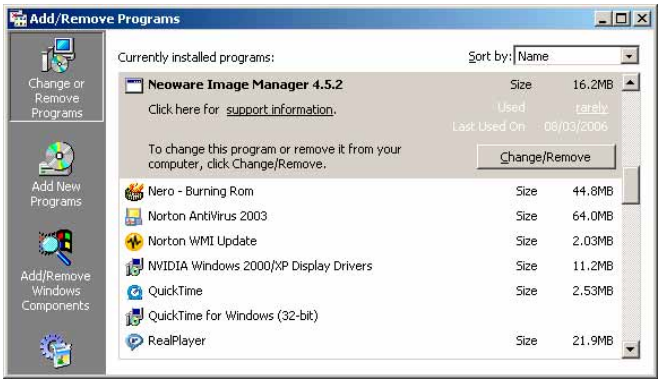
To stop the NVDD server module, press the keys **Ctrl** + **C**.

Uninstalling Neoware Image Manager

This section describes how to remove Neoware Image Manager from your computer. Note that it is possible to uninstall the Image Manager software from an Image Manager bootable drive. It will just uninstall the components that have been copied during InstallShield installation, but will not uninstall the components and configuration performed during Image Creation. In other words, you can uninstall the InstallShield package without making your virtual drive unbootable by Image Manager.

Uninstall Procedure

1 To uninstall Neoware Image Manager, select the **Add/Remove Programs** icon in the **Control Panel**.


Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by: Name
Neoware Image Manager 4.5.2
Size 16.2MB
Click here for support information.
Used rarely
Last Used On 08/03/2006
To change this program or remove it from your computer, click Change/Remove.
Change/Remove
Nero - Burning Rom Size 44.8MB
Norton AntiVirus 2003 Size 64.0MB
Norton WMI Update Size 2.03MB
NVIDIA Windows 2000/XP Display Drivers Size 11.2MB
QuickTime Size 2.53MB
QuickTime for Windows (32-bit)
RealPlayer Size 21.9MB

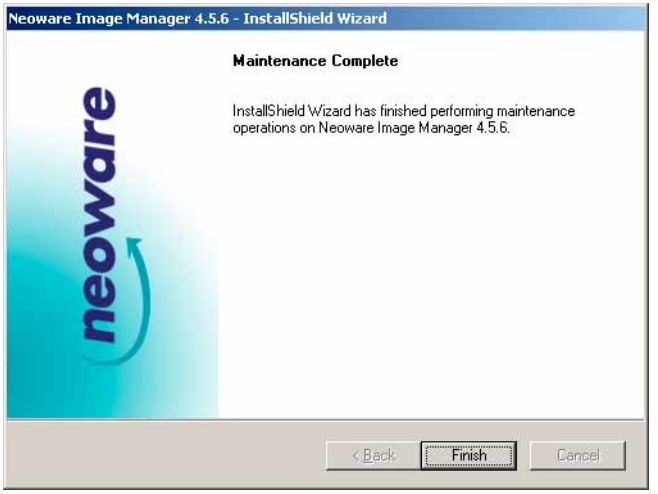
2 Select the **Neoware Image Manager** entry in the list of installed programs, then click the **Change/Remove** button. The InstallShield Wizard dialog will be displayed.

Neoware Image Manager 4.5.2 - InstallShield Wizard
Welcome
Modify, repair, or remove the program.
Welcome to the Neoware Image Manager 4.5.2 Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.
Modify
Select new program features to add or select currently installed features to remove.
Repair
Reinstall all program features installed by the previous setup.
Remove
Remove all installed features.
InstallShield
< Back
Next >
Cancel

3 Select **Remove** then click **Next**.

Neoware Image Manager 4.5.2 - InstallShield Wizard
Do you want to completely remove the selected application and all of its features?
Yes
No

4 A warning message will be displayed to check whether you really want to remove the software. Click **Yes** to start the remove software process.



5 When the InstallShield Wizard has completed removing the software, click **Finish**.

Undoing Client Builder Changes on an HDD-based Configuration

It is possible to undo the changes that Neoware Image Manager Client Builder has performed on an HDD based configuration, in case the creation process did not complete smoothly or was not closed neatly.

To undo changes:

1. Open a command prompt and navigate to the folder where the file `NeowareIMClientBuilder.exe` is installed (usually `C:\Program Files\Neoware\Image Manager 4.6\Client`.)
2. Enter the following command:

   ```
   NeowareIMClientBuilder.exe –r
   ```

The last dialogs of Neoware Image Manager Client Builder will be displayed and when it exists, Neoware Image Manager will undo every change it may have made to the local OS configuration, if such changes are still active in your OS. You will have to reboot in order for all these changes to be actually undone. A dialog asking you to reboot or shutdown will be displayed by Client Builder.

CHAPTER 4

Creating a Client Image

This chapter describes how to use Client Builder to create a client image on the Image Manager server.

Introduction

The Client Builder component of Neoware Image Manager makes a complete image of a system partition (hard disk) based on the size of the partition, not its contents. It is recommended that the size of the partition is adjusted once all software has been installed (using PowerQuest Partition Magic, for example). If the partition is too big then the image created from it will have a negative effect on manageability and make administration and backups more difficult. However, performance is not affected by partition size. The partition size should ideally be under 16 GB. If extra storage is required, you can use a network shared directory housed by a Windows, Samba or CIFS/SMB compatible server. It is also recommended that the partition is defragmented before the image is built.

Using Client Builder

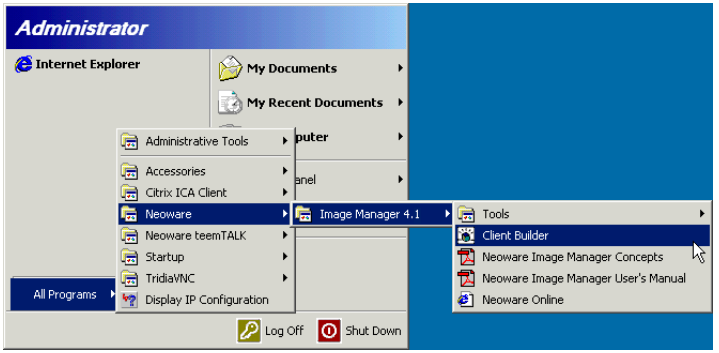
The following procedure assumes that you have already installed the **Client** components of the Neoware Image Manager on the hard disk drive that will be used to create the client image. You must be logged on as a user with administrator privileges.

1. Before running Client Builder you must *always* make sure the NVDD server module is running on the Image Manager server, and is serving a non-bootable virtual disk to the client running Client Builder. A non-bootable virtual disk called `SmallDisk` is supplied with Neoware Image Manager.
2. To launch the NVDD server module so that it serves the non-bootable virtual disk (e.g. `SmallDisk`) to all the clients, navigate to the directory containing NVDD then type one of the following at the command prompt:

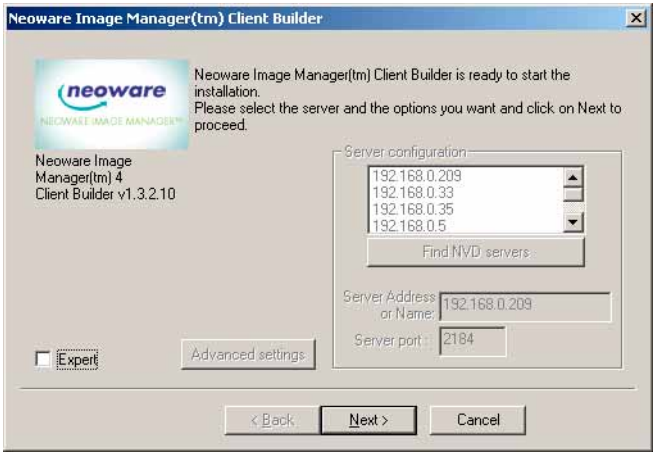
   Windows system: `nvdd -c nvdd.smalldisk.vol.conf`

   Linux/FreeBSD system: `./nvdd -c nvdd.smalldisk.vol.conf`
3. Close all applications on the *client* computer.
4. (Optional but recommended) Defragment the hard disk partition from which the image will be created using the **Defrag** utility.

   Note that you can defragment the virtual disk drive after it has been created by Client Builder.
5. Run Client Builder, either by launching the executable file `NeowareIMClientBuilder.exe`, or from the **Start** menu by selecting **Programs/Neoware/Image_Manager_4.6/Client Builder**.



The Client Builder dialog will be displayed.



6 If your server's IP address does not appear in the dialog, please verify that your Image Manager server is running, shares a non-bootable virtual disk such as `SmallDisk`, and both client and server can access the network.

Note that Client Builder finds the existing server on your network by sending server broadcast packets. If the server is behind a router, you will need to enter expert mode by checking the **Expert** box, then enter the **Server Address or Name**.

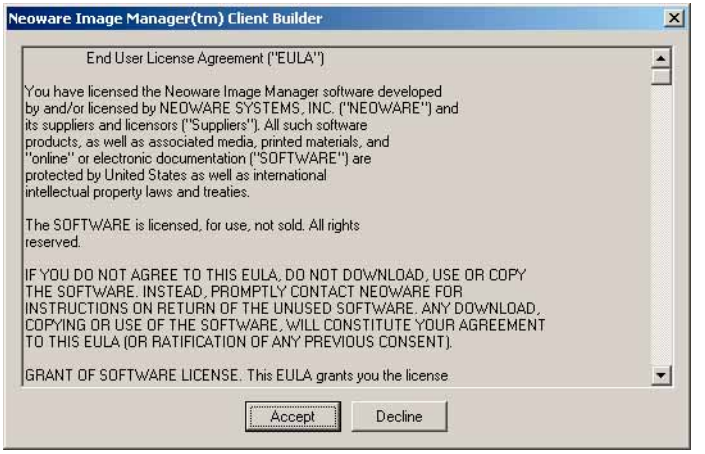
In order to enter the IP address manually, check the **Expert** box to access the options in the dialog. Enter the **Server Address or Name** of the server hosting Neoware Image Manager. Do not change the **Server port** default setting **2184** unless your server listens on a non-default port. Clicking the **Find NVD servers** button will enable you to search for the required server (using broadcast packets).

Clicking the **Advanced settings** button will display additional options. These should not normally be changed from the default settings. Refer to the section “Advanced Client Builder Options” on page 55 for details.

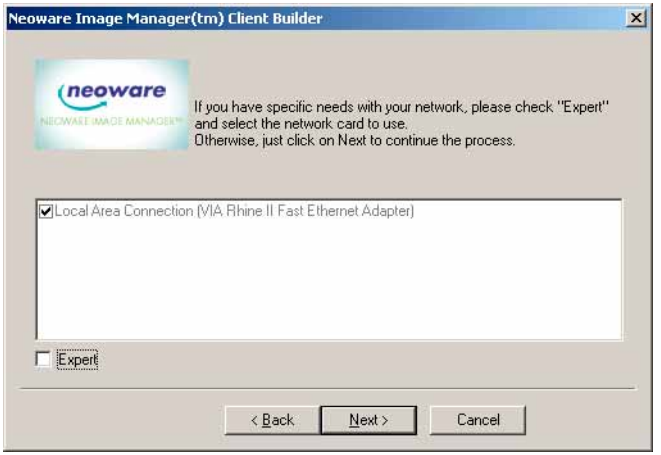
7 Click **Next** to continue.

Neoware Image Manager(tm) Client Builder
Client Builder is now ready to begin its installation. Before starting, please close all applications.
Do not use the computer while the image is being created.
If you wanted to defrag your partition before starting installation, please click on "no" button and launch defrag utility.
Proceed with installation?
Yes
No

8 An information message will be displayed. Click **Yes** to continue.


Neoware Image Manager(tm) Client Builder
End User License Agreement ("EULA")
You have licensed the Neoware Image Manager software developed by and/or licensed by NEOWARE SYSTEMS, INC. ("NEOWARE") and its suppliers and licensors ("Suppliers"). All such software products, as well as associated media, printed materials, and "online" or electronic documentation ("SOFTWARE") are protected by United States as well as international intellectual property laws and treaties.
The SOFTWARE is licensed, for use, not sold. All rights reserved.
IF YOU DO NOT AGREE TO THIS EULA, DO NOT DOWNLOAD, USE OR COPY THE SOFTWARE. INSTEAD, PROMPTLY CONTACT NEOWARE FOR INSTRUCTIONS ON RETURN OF THE UNUSED SOFTWARE. ANY DOWNLOAD, COPYING OR USE OF THE SOFTWARE, WILL CONSTITUTE YOUR AGREEMENT TO THIS EULA (OR RATIFICATION OF ANY PREVIOUS CONSENT).
GRANT OF SOFTWARE LICENSE. This EULA grants you the license
Accept
Decline

9 Read the license agreement then click **Accept** to continue.

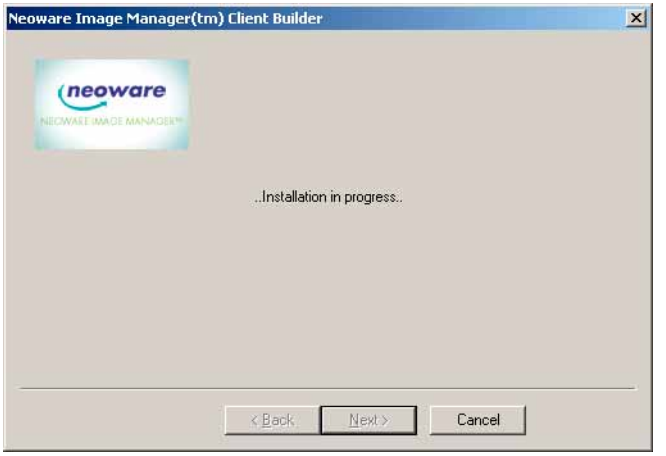

Neoware Image Manager(tm) Client Builder
neoware
If you have specific needs with your network, please check "Expert" and select the network card to use.
Otherwise, just click on Next to continue the process.
Local Area Connection (VIA Rhine II Fast Ethernet Adapter)
Expert
< Back
Next >
Cancel

10 A list of available network interface cards (NICs) will be displayed. This enables you to specify which NIC(s) to use to boot the client on Neoware Image Manager. All the available NICs are selected by default.

Check the **Expert** box to enable the tick box settings next to the listed NICs to be changed. You may select multiple NICs if this will be a multi-hardware image, but if you have multiple NICs in the same client you must only select one of them as the boot NIC. Note that you must select at least one NIC. Only Ethernet NICs are supported. WiFi NICs are not supported. If you select a WiFi NIC, your image will not be bootable using this NIC.

Tip: *If you intend to have many hardware clients booting off the same image, you may want to rename each NIC (in* ***Network Properties****) so that it is easier to find out which NICs to select.*

11 Click **Next.**



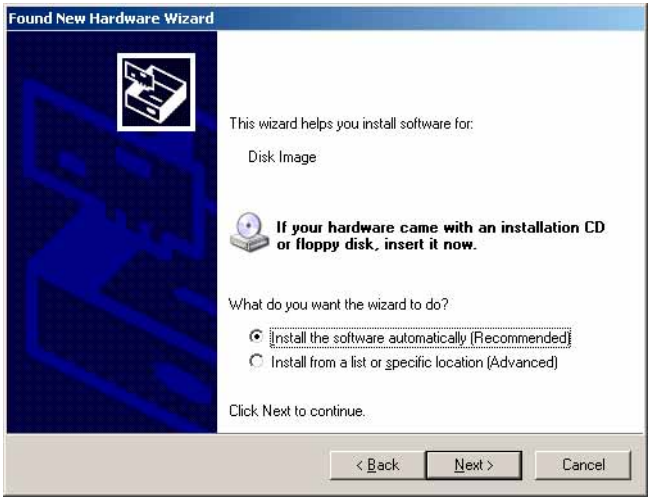
If your client OS is Windows XP SP2 and you have Windows XP Security Center enabled, you may be prompted that Automatic Windows Updates have been disabled. This is normal if you did not change Advanced Settings in the first step. You should not restore Automatic Windows Update (or any other Windows settings) before the image has been created. Client Builder will restore the original settings after it has completed.

12 On Windows 2000 and Windows XP you will see **Found New Hardware** wizard messages indicating the detection of new hardware (see the illustrations on the following pages). Just click on **Next** in each window until the driver installation has been completed, then click **Finish**.

Note: *Two "Neoware Emulated Disk Drive" devices may be detected. This is normal. If Windows asks you to reboot while installing one of these drivers, you must NOT reboot!*

Windows will tell you that the driver has not been digitally signed. Click the **Use Anyway** or **Continue** button when this message appears. You should then see some messages on the server side (in NVDD Server Module outputs) stating that the client has been detected.

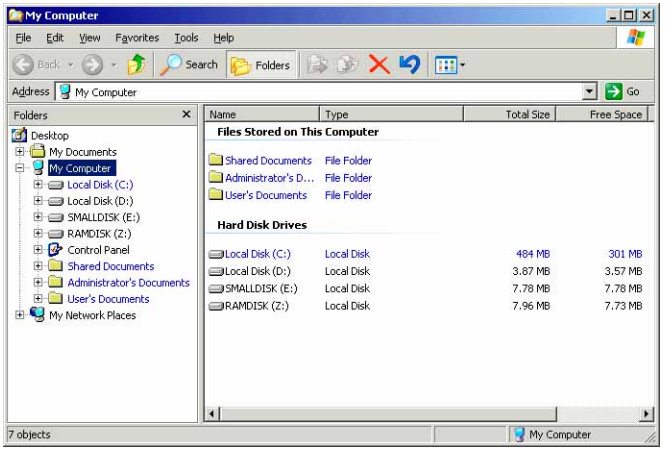
Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel


Found New Hardware Wizard
This wizard helps you install software for:
Disk Image
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

Hardware Installation
The software you are installing for this hardware:
Disk Image
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

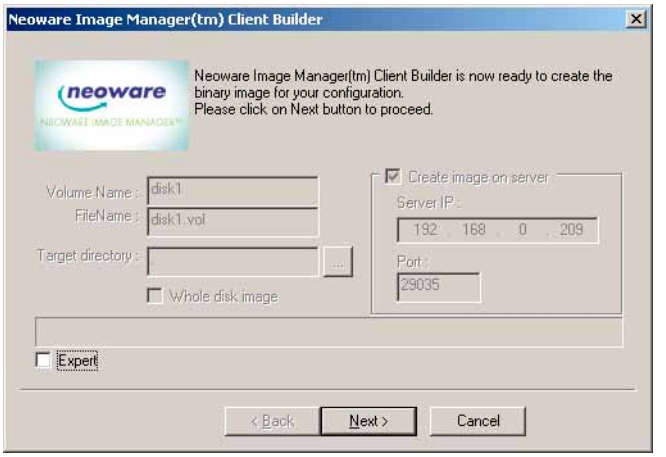
Click the **Continue Anyway** button.

13 Right-click on **My Computer** and select **Explore** in the pop-up menu. An additional hard disk called `SMALLDISK` should now be listed in the **My Computer** list of hard disk drives. For example:



You can also right-click on **My Computer** and select **Manage / Disk management** in the pop-up menu. If you do, ***do not do anything on this volume***, even if Windows proposes actions to be performed on it (for example: Initialize and Convert Disk wizard).

Wait for the **Found New Hardware** wizard to finish the installation, then click **Next**.


Neoware Image Manager(tm) Client Builder
neoware
NEOWARE IMAGE MANAGER
Neoware Image Manager(tm) Client Builder is now ready to create the binary image for your configuration.
Please click on Next button to proceed.
Volume Name : disk1
FileName : disk1.vol
Target directory :
Whole disk image
Create image on server
Server IP : 192 . 168 . 0 . 209
Port : 29035
Expert
< Back
Next >
Cancel

14 The Client Builder dialog is displayed with the volume name and server address automatically set by the system. If you need to change the entries in this dialog, check the **Expert** box to enable the options.

Note that the settings in the right half of the dialog use the internal protocol between Client Builder and the NVDD server module to create the image. The target directory will need to be set from the server's perspective so that the image is created in the correct server directory. Specifying "." as the target directory is the usual way to create the image file in the directory containing the NVDD server module.

You can enter a name for the hard disk volume to be created in the **Volume Name** box. This name will be used to identify the volume to the NVDD server module. The **Filename** box will automatically display the volume name entered but with the `.vol` extension. It is recommended that you do not change the filename.

You can specify the **Target directory** where the client hard disk image file will be created. Specifying "`./`" as the target directory is the usual way to create the image file in the directory where the NVDD server module is located.

When **Create image on server** is selected, the **Server IP** address and **Port** number will be automatically filled in by default using the information supplied earlier. A password may be needed if you have set one on the NVDD server using the NVDD Password utility.

When the **Whole disk image** option is *not* selected, Client Builder will build an image based on the first partition of the hard disk drive. It will contain the MBR (Master Boot Record) of the original hard disk drive with a modified partition table so that the virtual disk drive contains only one partition (the first partition).

If the system partition (usually **C:**) is not the first partition, the **Whole disk image** option will be selected by default. This

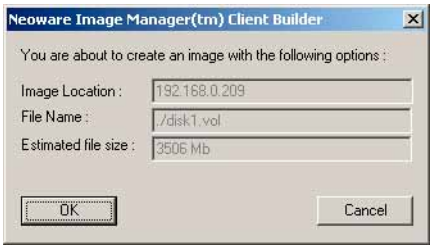
ensures that when Client Builder creates an image from an existing Neoware or ThinTune XPe flash disk, it will create the correct type of image.

If the system partition is the first partition, only the first partition (actually the MBR plus the first partition) will be used as the source of the image. Administrators using XP Pro booted from an actual hard disk drive will then, usually, create an image of their system (first) partition.

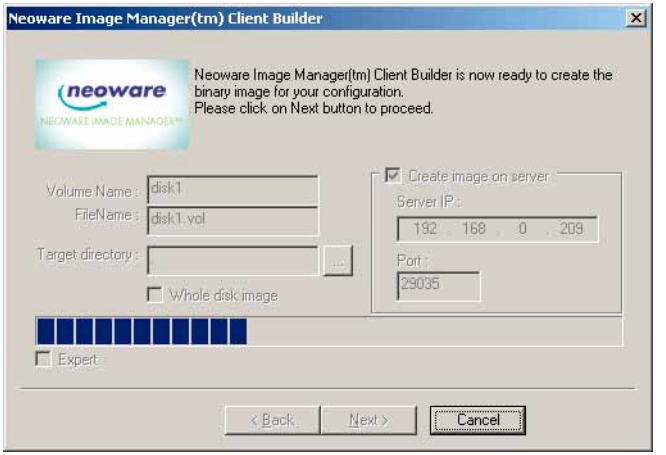
If you use **Expert** mode, you can also create the image as a regular file instead of using a special communication channel between the server and Client Builder. Just deselect the **Create image on server** option.

In this case the image file must be stored on another computer or, at least, a different partition to the one from which it is created. We recommend that the target directory is the one containing the NVDD server module (this implies that Samba server is installed on the NVDD server if it is not a Microsoft Windows server, or is not natively able to accept connections from remote clients in the Windows Networking fashion).

15 Click **Next** to display a confirmation dialog that summarizes the details of the image to be created. If the details are not correct, click the **Cancel** button to make the required changes.



16 Click **OK** to begin building the client hard disk image. It should take no more than 5 minutes per gigabyte (usually 3 minutes per gigabyte on a 100mb/s full duplex network). A progress bar will indicate the progress of the build.



Important: *When you create the image file on the server, if the image creation takes more than 5 minutes per gigabyte of partition, this implies that the global performance of your system is not adequate. You may then have problems when using diskless clients, especially when using several clients at the same time. You should investigate why the image creation is slow. Look for problems in the server hard disk, network, server resources and client network resources. You may increase performance with updated drivers for the server and client NIC and server HD controllers, and also with a defragmentation of the server drives before the image is created.*

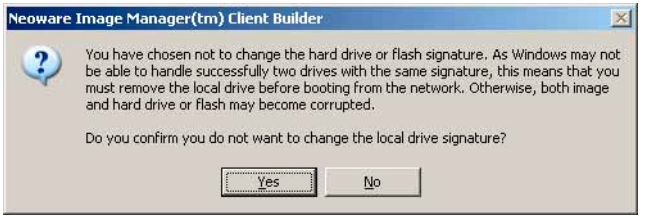
17 The following dialog will be displayed once the Client Builder has finished creating the image.

Neoware Image Manager(tm) Client Builder
neoware
NEOWARE IMAGE MANAGER
Neoware Image Manager(tm) Client Builder has now finished the creation of the image.
Click on Finish to restore the original configuration on your hard drive.
The image ClientBuilder created contains data strictly identical to the data in the original drive, including the disk signature. Windows may not be able to reliably handle disks with the same signature, nor detect such a situation. Thus you must:
- either ask Client Builder to change the signature on your hard (or flash) drive
- or physically disconnect the drive before booting from the network.
Otherwise, both image and hard (or flash) drive may become corrupted.
Change disk signature on local hard drive
Expert
< Back
Finish
Cancel

Client Builder has created an image that contains exactly the same data as stored on your original hard disk drive, including the disk signature. Windows may not be able to reliably handle two drives that have the same signature, nor detect such a situation in a manner that suits your requirements. Usually you will want the Virtual drive to be mounted as **C:**, but Windows will mount your Local hard disk drive as **C:** if its signature has not changed, making the Virtual drive mounted on another letter. As a result you must either ask Client Builder to change the signature on the Local drive, or physically disconnect the local drive before booting off the newly created image.

Note: *Changing the disk signature may have an impact on some operating systems where the license is based on the hardware. For example, you should not change the disk signature on a thin client using flash to boot from Windows XPe. If your client OS is XPe you MUST remove the local drive or flash before booting off the image created from the local hard disk drive or flash drive. In other cases there should be no problems in booting from a drive changed in this way.*

18 Click **Finish**. A message box will be displayed if you did not check the **Change disk signature on local hard drive** option.


Neoware Image Manager(tm) Client Builder
You have chosen not to change the hard drive or flash signature. As Windows may not be able to handle successfully two drives with the same signature, this means that you must remove the local drive before booting from the network. Otherwise, both image and hard drive or flash may become corrupted.
Do you confirm you do not want to change the local drive signature?
Yes
No

If you click **No**, the previous dialog will be displayed and you will be able to check the **Expert** box and configure Client Builder for it to change the local drive signature.

The following dialog will be displayed if you configured Client Builder to change the local drive signature:

Neoware Image Manager(tm) Client Builder
Caution: the signature modification is done on the local hard disk drive to enable its usage along with the created image, in order not to have two disk drives with the same signature. If you do not plan to leave the local hard disk drive installed in the computer, you do not need to change its signature.
Proceed?
Yes
No

Click **Yes** if you want to change the signature on the local drive. (If you click **No**, the previous dialog will be displayed and you will be able to change the Client Builder configuration so that it will not change the local drive signature.)

Client Builder will then display a dialog that summarizes what is left to be done in order for your clients to be able to boot off the newly created image.

Neoware Image Manager(tm) Client Builder
Client Builder has achieved image creation. The next steps to finish the installation are:
- shutdown the computer
- if you did not change the signature, unplug the disk or flash
- set the server to share the newly created image (it will be shared by default in Admin mode)
- boot the computer and let windows detect new hardware
- reboot the computer and make sure everything works fine
- stop the computer and let the image be shared in the write mode you wish
Then: boot every client computer from the network and let them start from this image!
OK

19 Click **OK**.

In order to restore the original configuration of your client OS, Windows needs to be stopped. This is required in order to completely remove all the drivers installed previously.

20 Click **Yes** to shutdown the client computer. If you click **No**, Neoware Image Manager Client drivers will not be completely removed from the local OS. They will be completely removed at Windows shutdown.

21 On the Neoware Image Manager server, shut down the NVDD server module:

Windows system: Press the keys **Ctrl + C**

Linux/FreeBSD system:
Either press the keys **Ctrl + C**, or send a `SIGINT` signal to `nvdd` from another shell (for example, by using the `killall` command with the appropriate parameters).

Two files will have been created by Client Builder in the target directory for the client hard disk image:

- a file containing the actual image (e.g. `disk0.vol`)
- a configuration file (e.g. `nvdd.disk0.vol.conf`)

You now need to configure the server in order for clients to be able to access the image. This is described in the chapter: “Enabling Clients to Access Images” on page 59.

Testing the Image

You can check that the image works correctly by running it on the Image Manager server as follows:

1. Run NVDD with the parameter:

   `-c nvdd.<image filename>.conf`

   For example:

   Windows: `nvdd.exe -c nvdd.disk0.vol.conf`

   Linux/FreeBSD: `./nvdd -c nvdd.disk0.vol.conf`

2. Check that the messages displayed are OK. If any error messages are displayed, relaunch NVDD with the extra parameter `-vall` to generate a complete log.

Advanced Client Builder Options

The Client Builder includes additional options for more advanced control over its operation. You can display these options by clicking the **Advanced settings** button in the initial dialog displayed when you run Client Builder.

You should not change the default settings in this dialog, except for the Virtual Memory settings, unless you are fully aware of the effect the changes will have.

All the settings in this dialog are only applied to the remote-booted operating system that will rely on the hard disk image to be created by Client Builder. They will have no impact on the operating system hosted by the Reference HD after Client Builder has completed.

Disable Autocheck at Startup

Default: Unchecked

This option prevents Windows from performing a ChkDsk command to check volume integrity at start-up.

Disable Windows Updates

Default: Checked

This option prevents Windows from using the Automatic Updates features. You should NOT uncheck this option unless you only use volumes mounted in Admin mode (i.e. a unique volume for each client computer).

If Automatic Updates are allowed when volumes are not mounted in Admin mode, they could make too many changes to the volume and cause the CVol write cache files on the server to become too big.

Administrators can perform Windows Updates manually by mounting the volume in Admin mode then using **Windows Update** in the **Start** menu.

Note that if this option is checked and your client is Windows XP with SP2 and has the Security Center enabled, after you chose the network cards to be used as Virtual Disk Drive Controllers, you may be prompted that Automatic Windows Updates have been disabled. This is normal. You should not restore Automatic Windows Updates (or any other Windows settings) before the image has been created. Client Builder will restore the original settings after it has completed.

Disable Daylight Saving

Default: Unchecked

This option prevents Windows from changing the system time according to daylight savings in certain countries. If this option is unchecked, Windows may change the system time at each boot when the boot volume is mounted in CVolwrite/Volatile mode. This is because the new time setting cannot be saved, so it will be lost on reboot.

Administrators can change the system time manually using BIOS settings, semi-manually using login scripts or startup scripts.

With Image Manager client, it is recommended that you use a tool that can automatically synchronize the client system time to another

system, such as an NTP server. For example, you can tweak the W32Time service according to the following document:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q223184

Disable Memory Dumps

Default: Checked

If Windows crashes, it tries by default to dump the crashed computer memory into a file that can be used later by experts to analyze the cause of the crash. With Neoware Image Manager clients, it is not normally necessary to retrieve these crash dump files, especially if the client computer is running in protected mode, because the dump file would be created and then deleted after a reboot.

Change Virtual Memory Settings

Default: Unchecked

This option, when selected, enables you to specify the size of virtual memory on the remote booted system. If you change it, it is recommended that the minimum and maximum virtual memory sizes are set to the same value, and that this value does not exceed the maximum CVol file size divided by 4.

XP Settings

These settings are specific to Windows XP clients and are not applicable to other client operating systems.

Disable Defrag During Screen Saver

Default: Checked

By default, Windows XP internal disk defragmenter will try to defragment the hard disk when the computer has been in an idle state for a certain time period. With Neoware Image Manager clients not using Admin mode, defragmentation must be avoided, otherwise the CVol write cache files will be filled up very quickly.

Defragmentation is only to be performed manually on volumes mounted in Admin mode.

Disable System Restore

Default: Checked

The System Restore feature enables users to restore a previous state of their hard disk. With Neoware Image Manager clients, system restore is usually not needed. It would use up disk space unnecessarily.

With Neoware Image Manager, if the system volume is opened in a protected mode, writes to this volume are not kept after a reboot. If the volume is mounted in Normal client mode, restoring the clean volume state is just a matter of deleting the corresponding CVol file.

System Restore would only be required with volumes mounted in Admin mode, when each client mounts its own volume.

Set Windows Prefetcher for Boot

Default: Checked

This decreases the time required to boot a client computer. You should leave this option checked.

Set Windows Prefetcher for Applications

Default: Unchecked

This increases the amount of data required to boot a client computer. You should leave this option unchecked.

CHAPTER 5

Enabling Clients to Access Images

This chapter describes how to configure the network and clients so that hard disk images can be accessed.

TFTP & DHCP Server Configuration

Before clients can access and boot from images on the Neoware Image Manager server, your TFTP and DHCP server must be configured to serve the Neoware Primary Bootstrap Loader file `mPXELdr.bin` to clients. This network boot program can be found in the `Server` directory of the Neoware Image Manager distribution package (for instance `C:\Program Files\Neoware\Image_Manager_4.6\Server`).

Windows

1. If you are already using standard Windows 2000/2003 TFTPD server, kill the TFTPD service (using the "Services" applet for instance).
2. Locate the following registry entry to specify the directory where the `mPXELdr.bin` file will be located:

   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tftpd\parameters\`*`directory`*

   Edit the *`directory`* if required. If some other files are to be served by TFTP, you will have to make sure that they are all in the directory specified by this parameter.
3. Start the TFTPD service again.

4 Copy the file `mPXELdr.bin` from the `Server` directory of the Neoware Image Manager distribution package, into the *`directory`* specified by the registry entry above.

(Neoware Image Manager includes a utility called TFTPD Installer that helps you to do this. Refer to the appendix "The TFTPD Installer" on page 293 for details.)

Note: *You can use any standard RFC compliant TFTP service. The freeware TFTPD32 (`http://www.jounin.net/`) for instance has been successfully tested with Neoware Image Manager.*

Linux/FreeBSD

The directory where files served by TFTP are stored is usually `/tftpboot` or `/tftproot`.

Copy the file `mPXELdr.bin` from the `Server` directory of the Neoware Image Manager distribution package, into the relevant directory where files served by TFTP are stored.

Make sure that the TFTPD daemon is configured correctly and working.

Testing the TFTP Service

You can test the TFTP service from a standard Windows 2000/XP/2003 PC by typing the following at the command prompt:

```
tftp -i <host_IP_address> get mPXELdr.bin %TEMP%\mPXELdr.bin
```

If the TFTP command fails, you need to rectify the problem before you can actually boot your clients from the network.

If the TFTP command succeeds, this means that the TFTP server is correctly configured to serve `mPXELdr.bin` (at least to the client that was used to launch this command). You can then delete the `mPXELdr.bin` file that has been copied to a temporary directory by entering the following commands:

```
attrib -r %TEMP%\mPXELdr.bin
del %TEMP%\mPXELdr.bin
```

DHCP Server Configuration

Configure your DHCP server so that it serves the file `mPXELdr.bin` to the clients. (Refer to the DHCP , TFTP and PXE documentation for details.)

If you use Microsoft Windows DHCP Server on a Windows 2000/ 2003 server, refer to the appendix “Configuring the DHCP Server” on page 297.

The DHCP/BOOTP `next-server` entry must be set to the TFTP server’s IP address.

Refer to the appendix “DHCP Reference” on page 317 for information on how clients locate the Neoware Image Manager server, and the DHCP options used.

Note: *The freeware TFTPD32 (`http://www.jounin.net`) embeds a simple DHCP server that has been successfully tested with Neoware Image Manager. TFTPD32 should then provide the TFTP and DHCP services on the same computer. If the computer that runs TFTP and DHCP services also runs NVDD service (Neoware Image Manager Server module), there is no need to configure extra DHCP options.*

Client Configuration

1. If the client contains a bootable hard disk drive or flash disk, either disable the disk or physically remove it.
2. Make sure the client is configured to boot with PXE (boot from LAN).
3. Start the client.

   The client's PXE PROM will display some messages. The Neoware Primary Bootstrap Loader file `mPXELdr.bin` is served to the client. The client then executes Neoware Primary Bootstrap Loader.

   Messages specific to Neoware Primary Bootstrap Loader are displayed, followed by a screen showing the Neoware logo.

   If a Windows Start menu was present on the original hard disk, it will be displayed. Windows is booted and you may be prompted to enter your login and password. Any login/password that could be used on the hard disk-booted client can also be used when remote booted.

Troubleshooting

If you experience any problems when the client boots, such as a blue screen or the client freezing, please do the following:

1. Power off the client. Wait for 1 minute. Power on the client again.
2. Check the NVDD server messages.
3. Power Off the client. Open its case and reconnect the original system boot drive to the IDE or SCSI and power cables, then boot the client from it.
4. Open the registry editor and, if they exist, remove the keys (and subkeys) in:

   `HKLM\System\CurrentControlSet\Enum\DSKIMG`
   (you may need to give full control authorizations to everyone on `DSKIMG` key and subkeys to be able to actually remove them)

   `HKLM\System\CurrentControlSet\CriticalDeviceData-base\diskimage`

   `HKLM\System\CurrentControlSet\Services\BDRUPD`

   `HKLM\System\CurrentControlSet\Services\DSKIMG`

   `HKLM\System\CurrentControlSet\Services\NeoDomMgr`

   `HKLM\System\CurrentControlSet\Services\NVD`
5. Run the Client Builder. Open the Device Manager and check for hardware changes. Wait until Client Builder finishes. Shutdown the client. Exit the `nvdd` process on the server. If required, copy the image file on the server (in the folder where NVDD is located). Make sure that NVDD configuration file (`nvdd.conf` by default) is OK for the image. Run `nvdd` again on the server. Remove the hard disk from the client. Start the client and boot it from LAN (PXE boot).

CHAPTER 6

Assigning Volumes to Clients

This chapter describes how to use the Image Manager Console to assign volumes to clients.

Introduction

This chapter describes how to use the Image Manager Console to assign volumes to clients. "Volume" is the name of the Virtual Disk Drive logical object. For a complete description of all the options available using the Console, refer to the chapter “The Image Manager Console” on page 181. For a description of the image configuration file that the Console modifies, refer to the chapter “The NVDD Configuration File” on page 213.

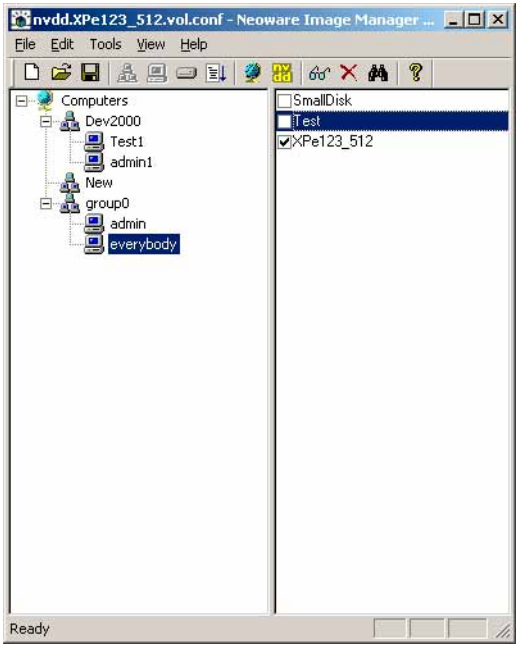
Running the Image Manager Console

The Image Manager Console enables you to create volumes and assign them to specific clients. The Console also provides a user-friendly way of accessing and changing the settings in a hard disk image’s configuration file (`nvdd.<image filename>.conf`) without having to use a text editor to manually edit it.

To run the Image Manager Console from the **Start** menu, select **Programs/Neoware/Image Manager 4.6/Neoware Image Manager Console**. You can also run the executable file `NIMConsole.exe`.

To open a Neoware Image Manager Server configuration file in the Console, display the **File** menu and select **Open**. Neoware Image Manager Server configuration files have the file extension `.conf`. You can also open a configuration file actually in use on a remote server by clicking the **nvdd** button in the tool bar. Refer to the chapter “The Image Manager Console” on page 181 for details.

When a Neoware Image Manager Server configuration file is opened in the Image Manager Console, the two panels will list the associated Clients and Volumes.



The Clients panel on the left displays the names of computers and groups of computers. The Volumes panel on the right displays the names of all the volumes (images) that can be assigned to the groups of computers.

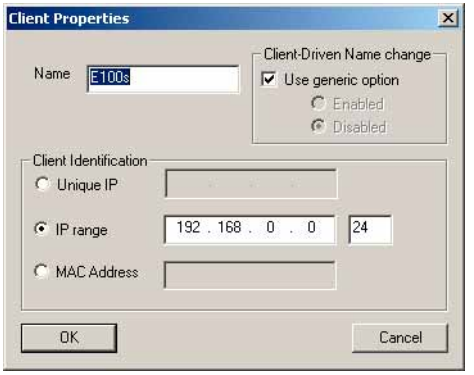
Each volume name has a check box next to it. This indicates whether the volume is assigned to the currently selected computer group. Selecting a computer name will indicate the volumes associated with

its group. You can easily select or deselect volumes for a specific group by selecting the name of the group (or a computer within it) then clicking the relevant volume check boxes.

If you want to make a computer a member of a group, just drag and drop the computer icon on the target group.

Adding New Clients

A Client object in the Image Manager Console can refer to a collection of computers on a subnet, not just a single workstation, connected to the Image Manager server. To add a new Client object to the Clients list, right-click either on the **Computers** item at the top of the panel, or on the name of the group to which you want to assign the new computer. Select **Create** then **Computer** in the pop-up menu. The **Client Properties** dialog will be displayed.



Specify a name for the client as it will appear in the Clients list. If you would like the client to be able to change and save the client name in the nvdd configuration file in the future, select the appropriate option for **Client-Driven Name Change** (refer to the section "Client-Driven Name Change" on page 190 for details).

Computers are identified either by specifying an IP subnet mask, full IP address (actually an IP subnet with a subnet mask of 32 bits) or a unique MAC address.

Typical subnet masks are:

32 This is the subnet mask for a single IP address.
For example, 194.199.93.24/32 means a range of 1 IP address (a single client computer).

24 254 IP addresses (a complete class C).
For example, 192.168.0.0/24 means all the IP addresses between 192.168.0.1 and 192.168.0.254.

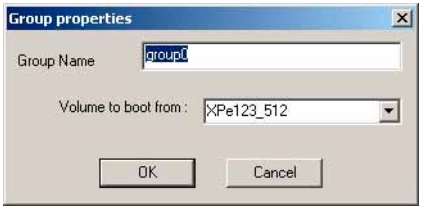
16 65534 IP addresses (a complete class B).
For example, 172.16.0.0/16 means all the IP addresses between 172.16.0.0 and 172.16.254.254.

0 Is usually only used with IP address 0.0.0.0.
0.0.0.0/0 means all the IP addresses.

If you want to make a Client object (that can actually be a group of workstations identified as belonging to a subnet) a member of a group, just drag and drop the computer icon on the target group.

Adding a New Group

Groups are used to link computers to volumes. To create a group, right-click on the **Computers** item at the top of the Console Clients panel, select **Create** then **Group** in the pop-up menu. The **Group Properties** dialog will be displayed.



Specify a name for the group then click **OK**.

After you have specified the volumes to be used by this group (as described in the next section), display the **Group Properties** dialog again to select the volume the group will use to boot from by default.

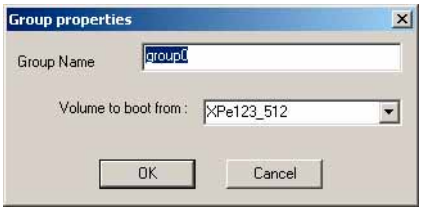
The drop-down list box will list all the bootable volumes currently associated with the group. Select the name of the default volume to boot from then click **OK**.

Note that if there are two or more bootable volumes associated with a group, when you switch on a client that belongs to that group, it will display a list of the volumes available to boot from. If you do not select a volume from the list, after ten seconds the client will automatically boot using the default volume specified here. (Refer to the section “Enabling Client MultiBoot” on page 235 for more details.)

Assigning a Volume to a Group

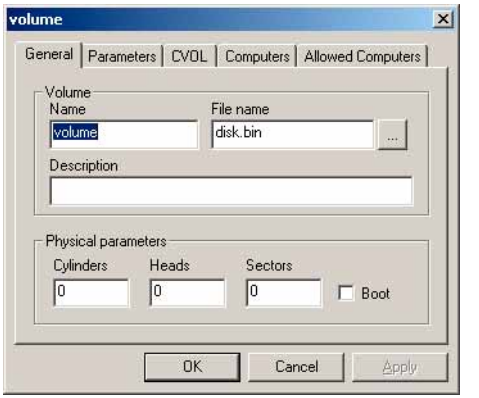
The name of each volume in the Console Volumes list has a check box next to it. This indicates whether the volume is assigned to the currently selected computer group in the Clients list. Selecting a computer name in the Clients list will indicate the volumes associated with its group. You can easily select or deselect volumes for a specific group by selecting the name of the group (or a computer within it) then clicking the relevant Volume check boxes.

Volumes can be shared by any number of computer groups and can be used as a boot disk or as storage. The volume used by a group to boot from is specified in the **Group Properties** dialog, which is displayed by double-clicking on the group name.



Creating or Modifying a Volume

You can create a new volume by right-clicking in the Volume panel and selecting **Create Volume** in the pop-up menu. You can modify an existing volume by double-clicking on the Volume item in the Volume panel, or by right-clicking on this item and selecting **Properties**. A dialog consisting of several tabs is displayed.



The **General** tab enables you to specify a name for the volume that will be used to identify it in the Console.

Specify the name of the hard disk image file to use in the **File name** box (click the **...** button to browse for it). Note that the file paths are relative to the location of the running nvdd server. This is particularly important to remember when you modify the configuration of a remote Image Manager server (then using the browse button is irrelevant).

The **Description** box enables you to provide a brief description of the volume which will be displayed on the client screen when it starts.

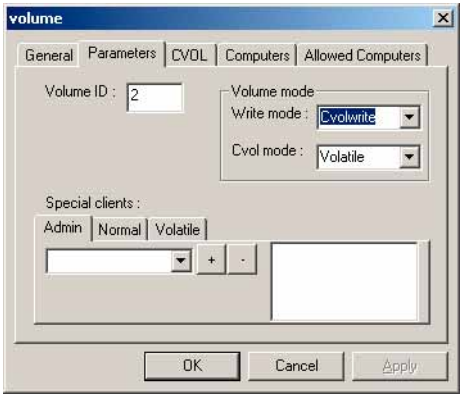
The **Physical Parameters** options enable you to specify the actual size of the volume and whether it is used as a boot drive or storage.

Heads: 255 (usually)

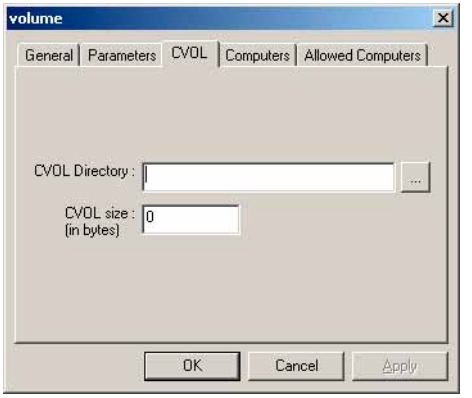
Sectors: 63 (usually)

Cylinders: (size of volume image (bytes) / (512 * heads * sectors)) + 1

Note that Client Builder will automatically provide the correct geometry parameters when it creates an image file and the associated configuration file.

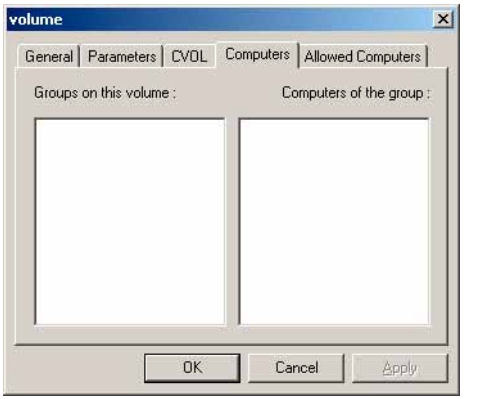


The **Parameters** tab enables you to specify the client writing mode for the volume and how it is shared. The **Volume Mode** settings enable you to specify the standard writing mode to be used, while the **Special Clients** options enable you to specify a different writing mode for individual clients. (For a description of the writing modes, refer to the section "Volume Write Modes" on page 82.) You can also specify a unique **Volume ID** number, but you should let Image Manager generate it automatically.

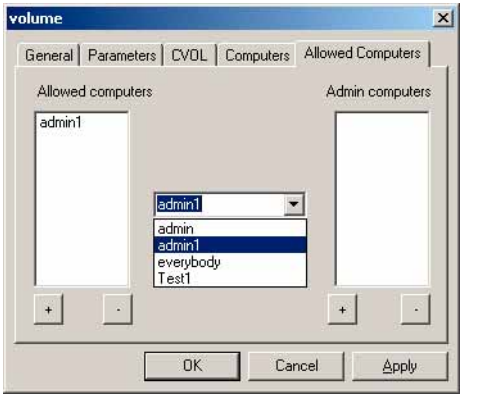


The **CVOL** tab enables you to specify a different directory for this volume's CVol files if they are not to be stored in the general CVol directory. Note that the file paths are relative to the location of the running nvdd server. This is particularly important to remember when you modify the configuration of a remote Image Manager server (then using the browse button is irrelevant).

You can also specify the maximum size of the CVol files if this maximum size is not the default one.



The **Computers** tab will display the names of all the computers that share this volume. (This is for information purposes only and not where you specify which computers share the volume.)



The **Allowed Computers** tab enables you to specify which computers are allowed to access this volume, and which computers are allowed in Admin mode.

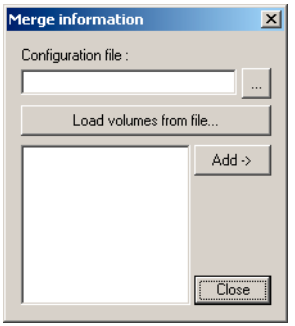
When you have finished specifying volume settings, click the **OK** button and the new volume name will appear in the Console Volumes list. You can now assign this volume to groups of computers.

Note: *Client Builder automatically creates a configuration file in which "everybody" (all the IP addresses in the world) can mount the created volume in Admin mode. We strongly recommend that you change this property after the first boot and when you are happy with the image, so that only trusted computers can mount a volume in Admin mode.*

Adding a Volume from Another Configuration File

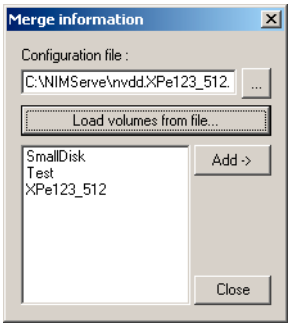
The Console enables you to open the configuration file of another hard disk image (i.e. a configuration file created using Client Builder) in order to copy volume definitions and parameters from it into the current configuration file.

Display the **Merge Information** dialog by selecting **Merge conf file** in the **Tools** menu.



Select the hard disk image configuration file containing the required volume definitions by using the **...** button to browse for it. Click the

Load volumes from file button to list the names of the volumes defined in the configuration file.



Select the volume you want to copy to the current configuration file then click **Add**. The volume will appear in the Console Volumes list. Repeat for each volume you want to add.

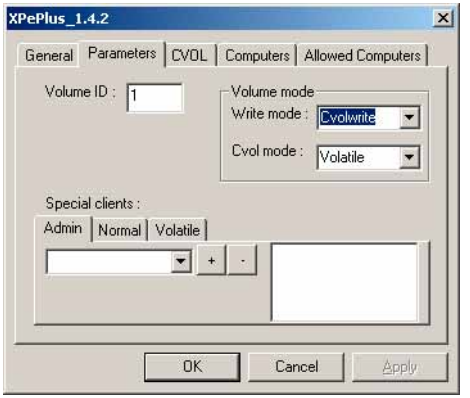
You must make sure that the properties of each copied volume specify the location of the hard disk image file associated with the configuration file currently being modified. To do this, double-click on the name of the volume to display the **Volume Properties** dialog, then change the path specified in **File name**, or browse to find the image file. Note that the file paths are relative to the location of the running nvdd server. This is particularly important to remember when you modify the configuration of a remote Image Manager server (then using the browse button is irrelevant).

Click **OK** to finish.

You may have to adjust the **Volume ID** in the **Volume Properties**, **Parameters** tab after you have added it.

Changing a Volume's Write Mode

You can quickly change the write mode of a volume. Just double-click on the name of the volume to display the **Volume Properties** dialog, then click on the **Parameters** tab.



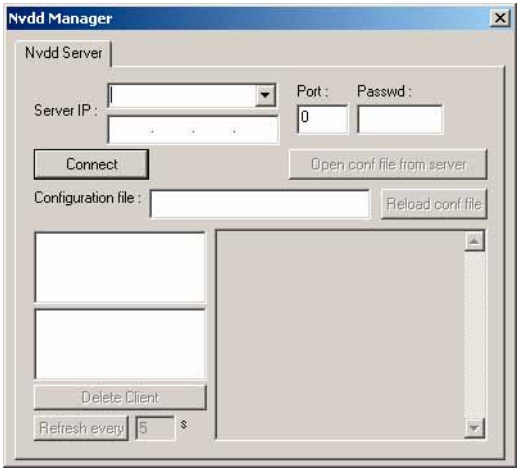
Change the **Volume Mode** (or **Special clients**) settings as required and click **OK**. (For a description of the writing modes, refer to the section "Volume Write Modes" on page 82.)

***Note:** If you select **Admin** for the **Write mode**, make sure the client computer you want to use in that mode is included in the list of Admin computers on the **Allowed Computers** tab.*

Modifying a Configuration File Currently Running

One of the most useful features of the Console is the ability to manage configuration files currently running, either on the local PC that runs the Console (if this PC also acts as a Neoware Image Manager server) or on remote Image Manager servers.

Selecting **Nvdd Manager** in the **Tools** menu will display the **Nvdd Manager** dialog. This enables you to connect to and manage Image Manager servers directly.

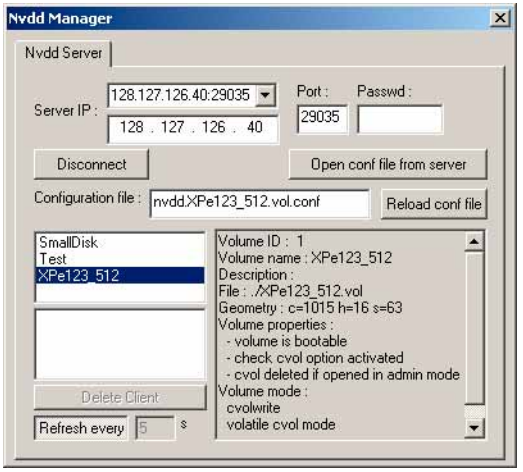


To connect to an Image Manager server, enter the server's IP address, port number (leave as 0 if using default port number on server side), and password if required, then click the **Connect** button. Note that the drop-down list contains the server addresses that have been used previously, so you can quickly select one of these.

If you want to connect to a Neoware Image Manager server that runs on the same PC that runs the Console, you can enter 127.0.0.1 as the IP address to connect to.

Note: *This method is the only one that can be used to actually modify a configuration file currently running. Editing the file (either using a text editor or with the Console using* ***File > Open****) is not possible as the configuration file is locked.*

When communication has been established with the remote server, the two list boxes on the left side of the dialog will show the volumes shared by the server and the clients currently communicating with it. You can select volumes or clients to obtain detailed information on them.



The name of the configuration file currently being used by the remote server is also displayed. You can edit this configuration file within the **Nvdd Manager** dialog by clicking the **Open conf file from server** button. When you have finished, **Save** the file. A message should indicate that the file has been correctly saved back on the server. You should then click the **Reload conf file** button to make the remote server take the changes into account.

Clicking the **Refresh every** button will update the contents of the dialog, otherwise the contents will be updated automatically after every number of seconds specified.

CHAPTER 7

Controlling the Use of Images & Volumes

This chapter describes the image configuration file settings that determine how clients can use images and volumes.

The Image Configuration File

With each hard disk image it creates, Client Builder also creates a corresponding configuration file that allows you to control how the image is used by clients. The configuration file is stored in the same directory as the image file and has the name `nvdd.<image filename>.conf`.

The Image Manager Console provides a user-friendly way of accessing and changing the settings in the `nvdd.<image filename>.conf` file without having to use a text editor to manually edit it. To run the Image Manager Console from the **Start** menu, select **Programs/Neoware/Image Manager 4.6/Neoware Image Manager Console**.

Note: *You may need to enter a password if you want to access configuration files on a remote Neoware Image Manager server.*

This chapter describes how to use the Image Manager Console to modify basic settings affecting the way images and volumes can be used by clients. The equivalent commands used in the `nvdd.<image filename>.conf` file are described in the chapter "The NVDD Configuration File" on page 213. A complete description of the Image Manager Console can be found in the chapter "The Image Manager Console" on page 181.

Client Volume Overlay Files

In the Image Manager system, a client mounts a server-based virtual disk drive (volume) consisting of a hard disk image file and a pair of Client Volume Overlay (CVol) files. The CVol files are created automatically by Neoware Image Manager Server based on settings in the hard disk image configuration file. Each client will have its own unique pair of CVol files: a header file that specifies how the client uses the volume, and a write overlay file used to store data written by the client.

The name of the CVol files incorporates the name of the hard disk image volume and the MAC address of the client. The data file will have the same name as the header file but with the file extension `.dat`.

`<VolumeName>@<ClientMACAddress>` (CVol header file)
`<VolumeName>@<ClientMACAddress>.dat` (CVol data file)

For example, a client using the volume named `testdisk` could have a pair of CVol files named as follows:

`testdisk@00E0C554E700` (CVol header file)
`testdisk@00E0C554E700.dat` (CVol data file)

The volume name that is used is the one defined in the server configuration file. It is usually the name of the image file without the `.vol` suffix.

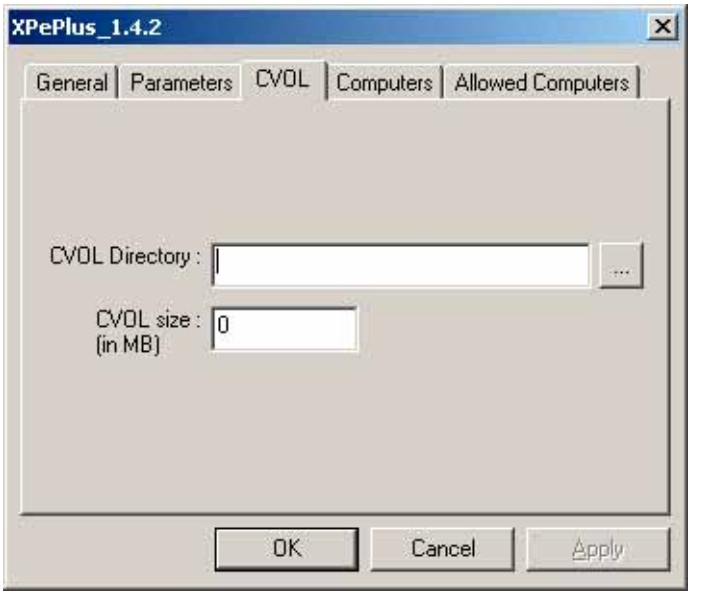
The CVol header file specifies the write mode that is used when the client mounts the volume. This mode affects the way in which data written by the client is handled. Refer to the section “Volume Write Modes” on page 82 for details.

You can merge the contents of a CVol data file with a hard disk image file in order to create a new hard disk image file. This is described in the chapter “Merging Image & CVol Files” on page 177.

Location of CVol Files

CVol files are stored in the same directory as the NVDD server module by default. You can specify a different general directory using the Image Manager Console by displaying the menu **Tools** > **Options** > **Generic Options**, then clicking on the **Directories** tab.

The CVol directory can be set relative to a specific volume, thus on a "per-volume" basis. This will take precedence over the general CVol directory setting. For example, the CVol files for `WinXP.vol` can be stored in `D:\temp\CVol`, and CVol files for `Win2K.vol` can be stored in `E:\ToBeSaved\CVols\Win2K.vol`.



If you run several NVDD processes on the same server on different ports, and have volumes with the same name in several configuration files currently in use, you should configure each NVDD to use a different folder to store CVol files. The same applies if you use "per volume" CVol folders.

Maximum Size of CVol Files

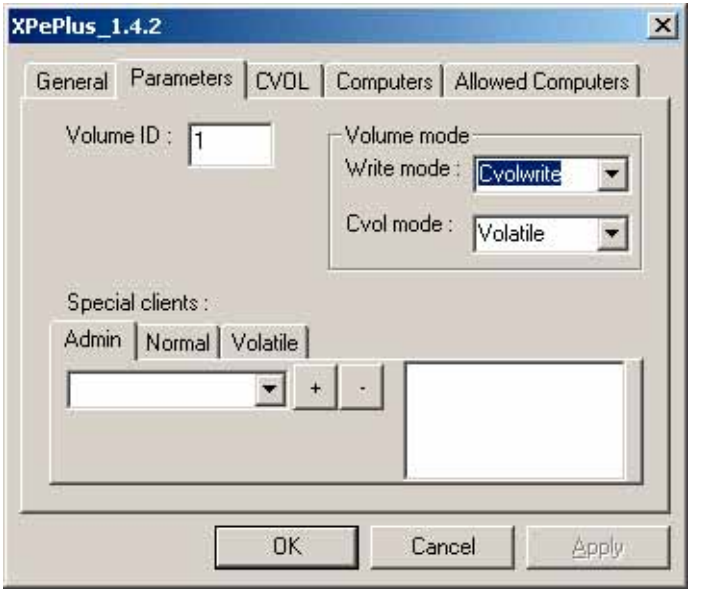
The default maximum size for CVol files can be specified by displaying the menu **Tools** > **Generic Options**, then the **General** tab. You can specify, on a per-volume basis, the maximum size that each

CVol file created for this volume can grow to using the Image Manager Console. Right-click on the Volume name, select **Properties** in the pop-up menu, then click the **CVOL** tab in the dialog. The **CVOL Size** setting determines the total number of megabytes that can be used by each CVol data file.

For more information on setting the CVol maximum size and what happens when the file becomes full, refer to the section "Maximum Size of CVol Files" on page 221.

Volume Write Modes

The volume write mode determines where data written by the client is stored and whether it is saved or lost on re-boot. The mode to be used when a client mounts a volume is specified in the Image Manager Console **Volume Properties** dialog, on the **Parameters** tab. To display this tab, right-click on the Volume name, select **Properties** in the pop-up menu, then click on the **Parameters** tab.



The **Volume Mode** settings enable you to specify the standard writing mode to be used when a client mounts the volume, while the **Special Clients** options enable you to specify a different writing mode for individual clients. You can also specify a unique **Volume ID** number, but you should let Image Manager generate it automatically.

There are two main write modes called Admin and CVolwrite. The CVolwrite mode consists of three submodes: Normal, Volatile and Persistent.

Admin Mode

Admin mode is used when you want to install a new application or make permanent changes to the hard disk image file. In this mode the client will write directly to the image file, not the CVol write cache file. The write is permanent.

Note the following:

- A volume can be mounted by only one client at the same time in Admin mode.
- No other client can mount a volume while it is being used by a client in Admin mode.
- No client can mount a volume in Admin mode if that volume is currently mounted by another client in any opening mode.

You can specify which clients are allowed to mount the volume in Admin mode by using the **Allowed Computers** tab.

CVolwrite Mode

In CVolwrite mode, all client writes will be directed to the client's own CVol data file. It has three submodes called Normal, Volatile and Persistent, that determine whether the write data is saved or lost on re-boot.

Normal Mode

Normal CVolwrite mode is used when you want the client to be able to install applications and make system changes without modifying the hard disk image file. Any application installations, system changes and disk writes made by the client are stored in the CVol

write cache file and will not be lost when the volume is re-mounted. This enables clients to have different configurations while sharing the same image file.

The CVol files can be sent to remote sites where an identical reference hard disk image file exists. This makes deployment of updated images to remote sites easier because you do not need to send a full-sized hard disk image. Note that the remote hard disk image will need to be updated using the `CVolMerge` tool.

The administrator can cancel all modifications made by the client user just by deleting the CVol files. The client will then mount the original unmodified volume again.

Important: *If any changes are made to the image file (e.g. using Admin mode), all the associated CVol files will be obsolete and Neoware Image Manager will usually automatically empty them.*

Volatile Mode

Volatile CVolwrite mode is used when you want the client to be able to use the volume without saving any client writes. Anything written to the CVol data file will be lost when the client is rebooted, thereby ensuring the volume configuration is exactly the same after each reboot. One of the advantages of this mode is that clients boot up from the server very quickly.

You can use Windows Roaming User Profiles (desktop, shortcuts, favourites, bookmarks, application settings, etc.) in Volatile mode. Roaming User Profiles are stored on a server and copied to the client volumes at logon time.

Persistent Mode

Persistent CVolwrite mode is similar to Volatile mode except that any client writes are replaced by a standard reference CVol content when the volume is mounted. When using this mode, the reference CVol content is created, for each client, at the first boot if it does not already exist. This enables you to specify a minimal safe customization for each computer (e.g. to retain Windows XP activation data customized for each computer). A complete description of this mode is provided in the section “Volume Write Modes” on page 82.

Note that if the hard disk image file is modified, the CVol files associated with it will be obsolete. Therefore Persistent mode should only be used when the original image file will not change often or when you can easily recreate persistent files after the image file has changed.

Tip: *As Neoware Image Manager Server automatically copies the reference CVol files to the actual CVol files to be used, it is recommended that the reference CVol files are compacted using the CVol-Compactor tool before they are actually used.*

CHAPTER 8

Adding Network Boot Devices to an Image

This chapter describes how to add bootable network card details to an image so it can be remote booted on different machines.

Overview

Neoware UbiBoot is a suite of tools that enable you to reduce the number of images required for a fleet of heterogeneous client hardware, making image management easier.

The UbiBoot Extractor and UbiBoot Inserter tools enable you to extract information about a bootable network interface card (NIC) and insert it into a Neoware Image Manager virtual disk. This allows the image to be remote booted on a collection of completely different machines.

The UbiBoot Extractor tool (`UBExtract.exe`) is run on the source machine containing the bootable NIC. It locates the active NIC, extracts information about it and stores it in a file within a directory. This directory is named `UbiBootData` by default and is located in the directory from which the UbiBoot Extractor program is run. You can change the location of this directory using the browse button at the top right of the UbiBoot Extractor window. The directory will be automatically created if it does not already exist. UbiBoot Extractor will *not* change the configuration or any registry items on the source machine.

The UbiBoot Inserter tool (`UBInsert.exe`) is run on the destination machine which *must* be running an existing Neoware Image Manager booted image, with the write-mode preferably configured as

'Normal' (an image with a CVol file that will still be accessible at the next reboot - the common image file itself must then be modified using the `CVolMerge` tool), or 'Admin' (we recommend that you create a backup copy of the image before making changes to it in Admin mode).

The UbiBoot Inserter dialog lists the descriptions of any bootable NIC data files stored in the `UbiBootData` directory to enable you to select the one to insert in the image. If the extracted data you want to insert are not in the default `UbiBootData` directory, you can select another directory using the browse button at the top right of the UbiBoot Inserter window. Clicking the **Insert** button once a selection is made will cause the information contained in the bootable NIC data file to be inserted either in the CVol file or the image file, depending on the writing mode of the virtual disk currently running.

Usually you would need to run UbiBoot Extractor and UbiBoot Inserter from the same operating system and service pack configuration. If the operating systems are too different then you might be able to extract and insert data, but the resulting image might not be bootable. When such a risk exists, UbiBoot Inserter displays the suspicious devices in red. For example, using UbiBoot Extractor on Windows 2000 sp4 then inserting the extracted data running UbiBoot Inserter on Windows XP sp2 is a hazardous operation for the Windows XP sp2 image. If you still decide to insert the data, UbiBoot Inserter will warn you that such an operation is not supported and will display a confirmation dialog requesting user confirmation.

UbiBoot Extractor and Inserter come with pre-extracted data for some Neoware thin clients, so that you do not even need to perform the extraction step to add hardware support for these devices into existing Neoware Image Manager virtual disks. Extra pre-extracted data may be available from Neoware technical support on request.

Before Using the UbiBoot Extractor & UbiBoot Inserter Tools

The data file created by UbiBoot Extractor must be stored in a workspace that is accessible by both source and destination machines. The workspace can be a USB key, a share on a networked machine, or any other storage that can be accessed by both machines. The user must have enough rights to create both directories and files.

We recommend leaving the `UBExtract.exe` and `UBInsert.exe` programs in the same directory on the workspace storage, and running them from there. By default UbiBoot Extractor will create the data file in a subdirectory of this directory, called `UbiBootData`. You can specify a different directory using the browse button at the top right of the window. When running UbiBoot Inserter from the same directory containing UbiBoot Extractor, it will automatically look for the data files for insertion in the subdirectory named `UbiBootData` located in the directory where UbiBoot Inserter is run from.

As both programs access restricted parts of the registry on their respective machines, they must be run from accounts with full administrative rights. Please note that being network administrator of an NT or Active Directory domain does not necessarily grant administrative rights on any local machine.

Note that UbiBoot Inserter will not accept being run from a non-Neoware Image Manager disk partition. There are two reasons for this restriction:

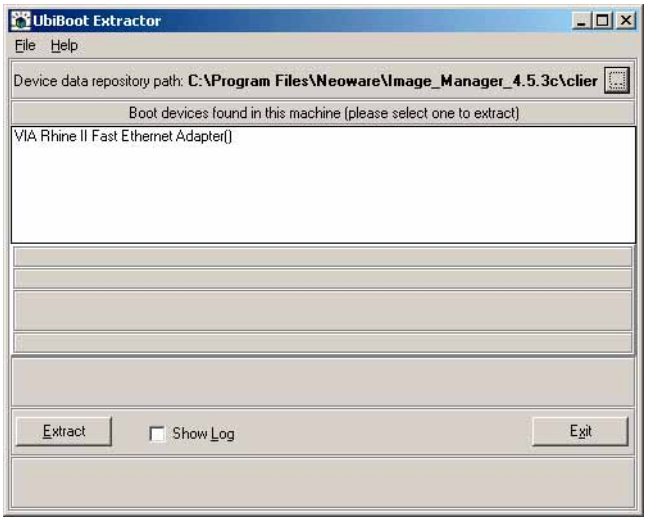
- UbiBoot Inserter expects to modify certain Neoware Image Manager-specific settings and will not be able to complete its insertion (and will fail) should this machine be locally booted.
- If the insertion operation fails or does not provide the expected results, it is far easier and faster to delete its CVol file, or to overwrite the copy of the virtual drive image file with the original image file, than to reinstall Windows on the destination machine then build an image again.

Extracting Boot Device Details

Note: *Before you perform the actual extraction process, we recommend that you update the Network Card Drivers on the computer whose hardware support is to be added to an existing Neoware Image Manager virtual disk.*

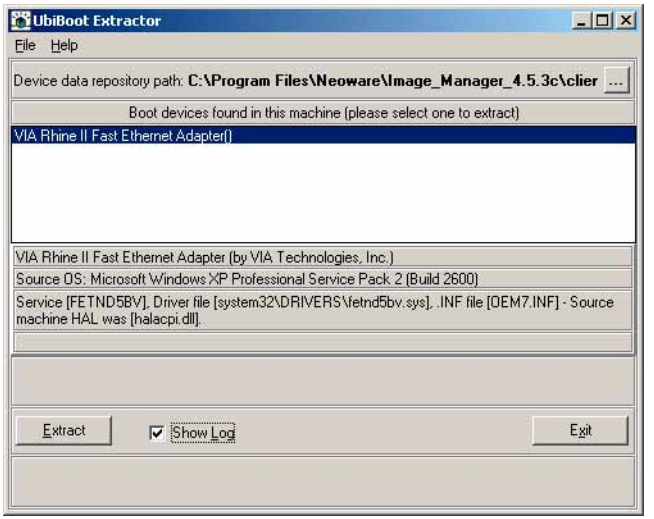
The following procedure will extract the details of a bootable network device and store the data in a file.

1. Select **Start** > **Neoware** > **Image Manager** > **Tools** > **UbiBoot Extractor**, or run the `UBExtract.exe` program on the machine from which hardware support is to be added to an existing Neoware Image Manager virtual disk. You must use an account that provides full administrative rights.



   UbiBoot Extractor will immediately detect and list the active NIC devices in the middle of the dialog.

Clicking on a device in the list will display a summary of its technical characteristics, such as its descriptive name and manufacturer, the OS of the machine containing the device (in this case, the OS currently running on the machine), and some file information that describes the device driver and environment.


UbiBoot Extractor
File Help
Device data repository path: C:\Program Files\Neoware\Image_Manager_4.5.3c\clier ...
Boot devices found in this machine (please select one to extract)
VIA Rhine II Fast Ethernet Adapter()
VIA Rhine II Fast Ethernet Adapter (by VIA Technologies, Inc.)
Source OS: Microsoft Windows XP Professional Service Pack 2 (Build 2600)
Service [FETND5BV], Driver file [system32\DRIVERS\fetnd5bv.sys], .INF file [OEM7.INF] - Source machine HAL was [halacpi.dll].
Extract
Show Log
Exit

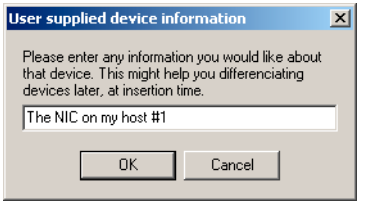
2. If you wish to use another repository other than the default one (subdirectory `UbiBootData`, located in the same directory where `UBExtract.exe` and `UBInsert.exe` are located), press the **...** button at the end of the **Device data repository** line near the top of the window. This will display a dialog that allows you to navigate to a different directory. If the path is too long for it to be displayed entirely, just leave your mouse pointer on it for a few seconds. A 'hint' box will be displayed with the complete path.
3. Select the device whose details you wish to extract, then click the **Export** button.

Note that if the device details have already stored as a file in the UbiBoot Extractor directory, the following dialog will be displayed.

Clicking **Cancel** will cancel the export operation.

Clicking **OK** will overwrite the information currently stored for this NIC with the latest information. This could be useful if a more recent revision of the NIC drivers have been installed, and the user wants to ensure that the latest version is inserted in the destination image. Note that if the manufacturer changed the internal code for the device from one revision to the next, UbiBoot Extractor will see the new NIC software revision as a different device and will record it in addition to the existing, older one.

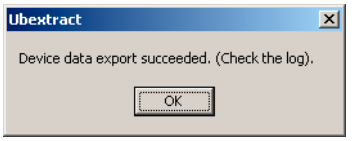
4 You will be prompted to enter descriptive text for this data file so you can identify it for selection using UbiBoot Inserter later. The descriptive text will appear between parentheses after the name of each NIC in the NIC list, as well as in the full description information of the selected NIC.


User supplied device information
Please enter any information you would like about that device. This might help you differenciating devices later, at insertion time.
The NIC on my host #1
OK
Cancel

5 Either enter a description then click **OK**, or click **Cancel** to continue with no description. (Entering a description is optional but highly recommended!)

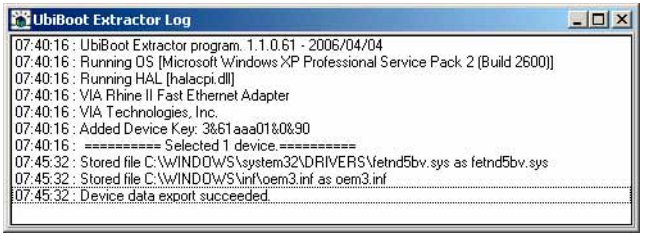
All the information about the currently selected NIC will be saved in a file in the repository directory. By default the name of the file is the complete PCI ID of the network adapter with the `.DEV` extension. For example: `VEN_14E4&DEV_167D&SUBSYS_05771014&REV_11-4&111a1fd8&0&00E0.Dev`. You can rename this file but you must keep the `.DEV` extension.

6 The following dialog will be displayed when the operation has been completed successfully.



If there was an error, a dialog will be displayed and a red error message will appear at the bottom of the UbiBoot Extractor main window.

You can display log messages in a separate window by checking the **Show Log** checkbox.


UbiBoot Extractor Log
07:40:16 : UbiBoot Extractor program. 1.1.0.61 - 2006/04/04
07:40:16 : Running OS [Microsoft Windows XP Professional Service Pack 2 (Build 2600)]
07:40:16 : Running HAL [halacpi.dll]
07:40:16 : VIA Rhine II Fast Ethernet Adapter
07:40:16 : VIA Technologies, Inc.
07:40:16 : Added Device Key: 3&61aaa01&0&90
07:40:16 : ========== Selected 1 device. ==========
07:45:32 : Stored file C:\WINDOWS\system32\DRIVERS\fetnd5bv.sys as fetnd5bv.sys
07:45:32 : Stored file C:\WINDOWS\inf\oem3.inf as oem3.inf
07:45:32 : Device data export succeeded.

The log messages can be saved in a file by selecting **Save Log** in the **File** menu, or by copying and pasting them into a word processor.

7 Click the **Exit** button to leave the program.

IMPORTANT NOTE

Starting with version 1.2 of the UbiBoot Extractor/Inserter programs, the original date and time of the driver files (typically the `.INF` and `.SYS` files) are preserved across extraction and insertion. Previous versions did not preserve the original date and time, and the files were marked as last modified at the time they were inserted.

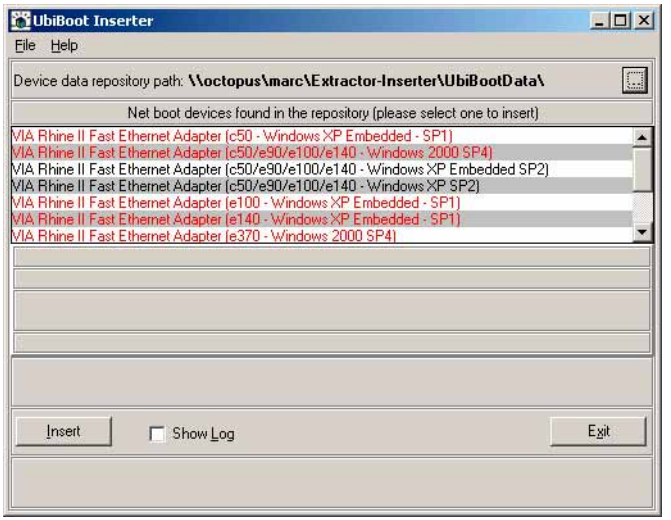
The `.DEV` files stored in the UbiBoot Extractor/Inserter repository are fully compatible between the 1.2 and pre-1.2 versions, but the pre 1.2 versions did not record the timestamps of the original files. If you use a 1.2 (or later) UbiBoot Inserter program with pre-1.2 `.DEV` files, the inserted files will now have the timestamp of the UbiBoot Extractor operation.

If you wanted to preserve the timestamp of the original files, you would have to recreate the `.DEV` files in your repository from the *original* driver files. In other words, extract all the devices using UbiBoot Extractor 1.2 or later again, then insert them using UbiBoot Inserter 1.2 or later.

Inserting Boot Device Details into an Image

The following procedure will insert the details of a bootable network device in a Neoware Image Manager image.

1 Select **Start** > **Neoware** > **Image Manager** > **Tools** > **UbiBoot Inserter**, or run the `UBInsert.exe` program on a machine booting off the disk image in which the bootable NIC data is to be inserted. You must use an account that provides full administrative rights.


UbiBoot Inserter
File Help
Device data repository path: \\octopus\marc\Extractor-Inserter\UbiBootData\
Net boot devices found in the repository (please select one to insert)
VIA Rhine II Fast Ethernet Adapter (c50 - Windows XP Embedded - SP1)
VIA Rhine II Fast Ethernet Adapter (c50/e90/e100/e140 - Windows 2000 SP4)
VIA Rhine II Fast Ethernet Adapter (c50/e90/e100/e140 - Windows XP Embedded SP2)
VIA Rhine II Fast Ethernet Adapter (c50/e90/e100/e140 - Windows XP SP2)
VIA Rhine II Fast Ethernet Adapter (e100 - Windows XP Embedded - SP1)
VIA Rhine II Fast Ethernet Adapter (e140 - Windows XP Embedded - SP1)
VIA Rhine II Fast Ethernet Adapter (e370 - Windows 2000 SP4)
Insert
Show Log
Exit

A dialog very similar to that of the UbiBoot Extractor tool will be displayed. It will list the descriptions of device data files created by UbiBoot Extractor that are currently stored in the `UbiBootData` directory. If you wish to use another repository other than the default one, press the **...** button at the end of the **Device data repository** line near the top of the window. This will display a dialog that allows you to navigate to a different directory. UbiBoot Inserter will then scan the specified directory and display the descriptions of device data files stored in it. If the path

is too long for it to be displayed entirely, just leave your mouse pointer on it for a few seconds. A 'hint' box will be displayed with the complete path.

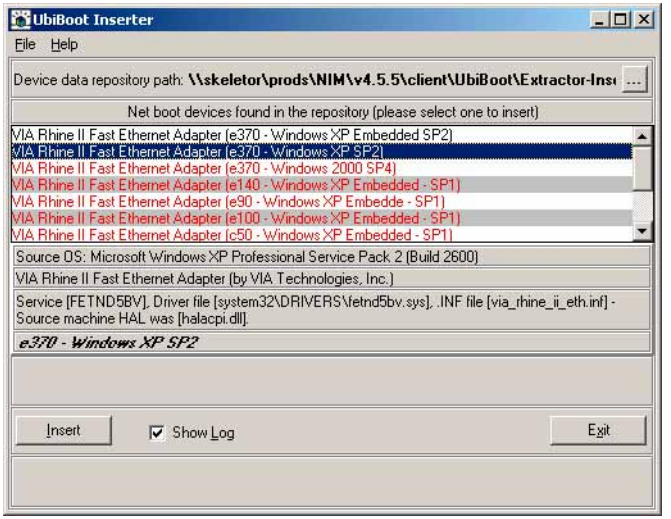
In the device list, any device that was extracted from a machine environment that is not strictly compatible with that of the current machine will appear in red letters. If the UbiBoot Extracted file came from a different OS, or an OS with a different service pack, or a machine running a different HAL (Hardware Abstraction Layer), it is hazardous to insert it in the current machine. Inserting such a device is possible, but is not supported. If the operation is attempted anyway, UbiBoot Inserter will display a confirmation dialog and request user confirmation before actually inserting the device.

Note: *If you launch UbiBoot Inserter when the destination machine is not running from a Neoware Image Manager virtual disk, the following message will appear at the bottom of the dialog:*

Can only insert into an NVD image.

In this situation, while it is still possible to browse the device repository, the ***Insert*** *button is disabled and the only possible option is to click the* ***Exit*** *button.*

2 Selecting a device description will cause the information that UbiBoot Extractor obtained from that NIC to be displayed below the device list.


UbiBoot Inserter
File Help
Device data repository path: \\skeletor\prods\NIM\v4.5.5\client\UbiBoot\Extractor-Ins
Net boot devices found in the repository (please select one to insert)
VIA Rhine II Fast Ethernet Adapter (e370 - Windows XP Embedded SP2)
VIA Rhine II Fast Ethernet Adapter (e370 - Windows XP SP2)
VIA Rhine II Fast Ethernet Adapter (e370 - Windows 2000 SP4)
VIA Rhine II Fast Ethernet Adapter (e140 - Windows XP Embedded - SP1)
VIA Rhine II Fast Ethernet Adapter (e90 - Windows XP Embedde - SP1)
VIA Rhine II Fast Ethernet Adapter (e100 - Windows XP Embedded - SP1)
VIA Rhine II Fast Ethernet Adapter (c50 - Windows XP Embedded - SP1)
Source OS: Microsoft Windows XP Professional Service Pack 2 (Build 2600)
VIA Rhine II Fast Ethernet Adapter (by VIA Technologies, Inc.)
Service [FETND5BV], Driver file [system32\DRIVERS\fetnd5bv.sys], .INF file [via_rhine_ii_eth.inf] - Source machine HAL was [halacpi.dll].
e370 - Windows XP SP2
Insert
Show Log
Exit

3 Click the **Insert** button. If the device was marked in red in the list (the OS or HAL (Hardware Abstraction Layer) of the source and destination machines are not identical), the following confirmation message(s) will pop up:

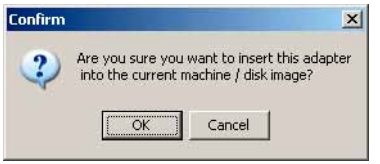
Warning
Warning:
Source and destination machines have different OSes.
Source device OS:
Microsoft Windows 2000 Professional Service Pack 4 (Build 2195)
Destination OS (this machine):
Microsoft Windows XP Professional Service Pack 2 (Build 2600)
Insertion of this device might be attempted, but is hazardous and UNSUPPORTED.
OK

Even if the same NIC device drivers could be used on the source and destination machines, extracting and inserting are only supported on source and destination machines that:

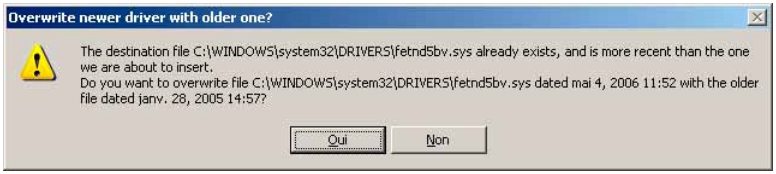
- run the same OS, service pack included. For example, extracting from Windows XPe (XP Embedded) and inserting in Windows XP Pro might damage the destination image to the point that a later successful, valid, same OS insertion will result in a machine that will not be able to boot from the inserted NIC.
- have the same basic architecture (for instance, extracting from a dual CPU machine and inserting into a single CPU machine might result in different HALs being used by the source and destination OS).

Clicking the **OK** button after this warning still allows the operation to continue, though, because the insertion may succeed in some cases.

4 Click the **Insert** button and accept the confirmation message to enter the device information in the target system configuration.



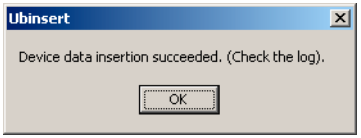
If the device files that you are about to insert into the NVD image are older than the device files in the current (destination) machine, warning and confirmation messages similar to the following will appear:


Overwrite newer driver with older one?
The destination file C:\WINDOWS\system32\DRIVERS\fetnd5bv.sys already exists, and is more recent than the one we are about to insert.
Do you want to overwrite file C:\WINDOWS\system32\DRIVERS\fetnd5bv.sys dated mai 4, 2006 11:52 with the older file dated janv. 28, 2005 14:57?
Oui
Non

This message might be displayed twice, once for the device `.INF` file and once for the device `.SYS` file. Note that if the device already in the machine was created using a version of UbiBoot Extractor/Inserter earlier than 1.2, the file time/date of the file(s) already present in the machine might reflect the date of the latest insertion, rather than the actual driver file release date. In this case, it is probably safe to accept to overwrite the existing file.

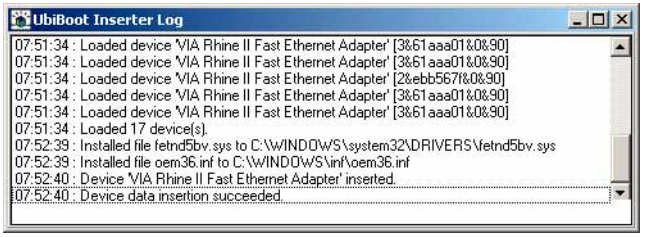
Our recommendation is to always keep the newest `.SYS` and `.INF` file.

5 The following dialog will be displayed when the operation has been completed successfully.



If there was an error, a dialog will be displayed and a red error message will appear at the bottom of the UbiBoot Inserter main window.

You can display log messages in a separate window by checking the **Show Log** checkbox.


UbiBoot Inserter Log
07:51:34 : Loaded device 'VIA Rhine II Fast Ethernet Adapter' [3&61aaa01&0&90]
07:51:34 : Loaded device 'VIA Rhine II Fast Ethernet Adapter' [3&61aaa01&0&90]
07:51:34 : Loaded device 'VIA Rhine II Fast Ethernet Adapter' [2&ebb567f&0&90]
07:51:34 : Loaded device 'VIA Rhine II Fast Ethernet Adapter' [3&61aaa01&0&90]
07:51:34 : Loaded device 'VIA Rhine II Fast Ethernet Adapter' [3&61aaa01&0&90]
07:51:34 : Loaded 17 device(s).
07:52:39 : Installed file fetnd5bv.sys to C:\WINDOWS\system32\DRIVERS\fetnd5bv.sys
07:52:39 : Installed file oem36.inf to C:\WINDOWS\inf\oem36.inf
07:52:40 : Device 'VIA Rhine II Fast Ethernet Adapter' inserted.
07:52:40 : Device data insertion succeeded.

The log messages can be saved in a file by selecting **Save Log** in the **File** menu, or by copying and pasting them into a word processor.

6 Click the **Exit** button to leave the program.

Note: *It is possible (although completely useless and strongly discouraged) to inject the same NIC information multiple times on the same machine. This only results in filling the system configuration of the destination machine with unnecessary data.*

The reason such an extraneous action is not blocked by UbiBoot Inserter is that the newly inserted NIC data might be subtly different from previous (and presumably obsolete) similar information, and UbiBoot Inserter cannot check if an identical set of data is being inserted yet again. It is thus up to the user of the UbiBoot Extractor and Inserter programs to use them appropriately.

Testing the Image

When the Neoware Image Manager virtual disk on the destination machine has been correctly modified by UbiBoot Inserter, you must validate that the source machine can actually be booted off that image:

1. If you were using CVolwrite/Normal mode on the destination machine, you might:

   - rename or copy the CVol files to associate them with the source machine. This implies that you already know the MAC address of the source machine that is to be included in the CVol file names. Refer to the section "Client Volume Overlay Files" on page 80 for details.
   - use `CVolMerge` to merge the changes in the destination machine's CVol files into the HD image file.

   If you had booted the destination machine in Admin mode, do not forget to switch back to either CVolwrite/Volatile mode or CVolwrite/Normal mode.

2. Boot test the source machine and the destination machine. Both should now boot. The instance of Windows that booted the source machine should now detect, configure or offer to configure all of its "new hardware".

3. If the source machine has successfully booted, it is now possible to add this enhancement to the HD image:

   Shutdown the source and the destination machines and change the writing mode to Admin or CVolwrite/Normal.

   Boot the source machine off the virtual drive and let Windows detect and install the hardware in the usual way. Re-boot each time Windows asks you to.

   When Windows has successfully detected all the hardware, if you were using CVolwrite/Normal mode, you may now want to commit the changes that are in the CVol files into the HD image

itself using the `CVolMerge` tool and, optionally, the `CVolCompactor` tool (if you intend to deploy the CVol file to remote locations, for instance).

The image has now been enhanced and you can now switch back to CVolwrite/Volatile mode.

CHAPTER 9

Building a Virtual Hard Disk to Boot any PC or TC

This chapter describes how to use Neoware UbiBoot to build a virtual hard disk that can boot a range of PC and TC configurations.

What is Neoware UbiBoot?

Neoware UbiBoot is a suite of tools that enable you to reduce the number of images required for a fleet of heterogeneous client hardware, making image management easier.

Neoware UbiBoot makes it possible to build a hard disk-based configuration that contains the hardware drivers for different PC and TC hardware configurations, thus rendering that configuration bootable from those PCs and TCs. Booting a PC or a TC from a UbiBoot-enabled configuration (cloned onto a hard disk using Neoware Active Cloner) will cause Windows to boot using compatible drivers for core hardware components such as PCI bus, IDE drives, CPU, video, etc. Once booted using these drivers, Windows will then detect the actual hardware devices and install the specific drivers. An image of that modified configuration will then boot Windows 2000, Windows XPe or Windows XP Pro on those two different hardware configurations.

Thus, Neoware UbiBoot offers an alternative to the use of UbiBoot Extractor and UbiBoot Inserter, with eventually the same objective.

UbiBoot can be used to create a variety of Windows installations:

- Create a hardware-independent Windows installation containing operating system, hardware drivers and applications which can be used on any hardware configuration. The hardware will be detected and configured when Windows boots.
- Create a Windows installation containing all the hardware drivers for a variety of PC configurations, then build a master hard disk image for deployment.
- Configure Windows on a Neoware Image Manager Virtual HD to recognize unknown hardware.

Installing Neoware UbiBoot

Neoware UbiBoot is installed when you perform a **Client** installation using the InstallShield Wizard as described in the chapter "Installing Image Manager Components" on page 19. Neoware UbiBoot must be installed on a regular IDE hard disk drive that stores a correctly configured instance of Windows 2000, Windows XP or Windows 2003 Server in partition **C:**. The contents of this hard disk drive will form the basis of the hard disk image that will be created later.

Note: *SCSI hard drives can be supported, but the detection of the SCSI controllers must be performed while Windows is booted off an IDE hard drive. SATA controllers are usually treated as IDE controllers and can be used directly.*

In order to achieve the most efficient results, the following points should be noted when you want to build a Windows system configuration that can run on heterogeneous hardware:

- Use the oldest computer in your fleet to perform the reference Windows installation (the installation that, after having been patched with Neoware UbiBoot, is to be deployed on several PCs and TCs). Refer to the section "HAL Considerations" on page 113 for more details about this.

- Start with a freshly formatted hard disk containing a clean installation of Windows. Note that Pre-installed Windows setups often embed proprietary components that may not be compatible with all the hardware configurations your Windows installation may need to run on. Pre-installed Windows setup should not be used as the base for a Neoware UbiBoot-enabled configuration.
- Avoid installing hardware-specific applications if the corresponding hardware is not present in every computer that will run with this installation of Windows. For example, the software modules `THOTKEY` or `TfcnKy` that are used to associate programs to some Toshiba Laptops extra keyboard keys may use up to 98% of CPU time when running on a non-Toshiba computer.

Note that because of the Plug'N'Play capabilities of Windows 2000/XP/2003, a hardware driver specific to a device on one PC can be installed on the Neoware UbiBoot enabled hard disk even if another PC or TC which does not have that device will be using the hard disk image. The operating system of the PC or TC will not be compromised as Windows will only invoke the device driver if the hardware is actually detected.

For information on HAL and ACPI, refer to the sections "HAL Considerations" on page 113, and "Mixing ACPI & Non-ACPI Computers" on page 115.

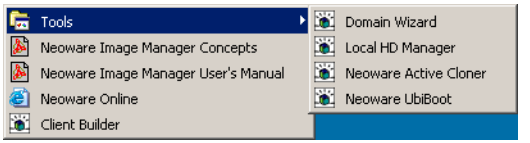
Potential Incompatibilities

It may not always be possible to create a single image that can boot all your hardware. Some drivers can be incompatible with each other, or with a piece of hardware. In this case it is recommended that several different images are created, one for each set of clients that can share a common disk image.

Running Neoware UbiBoot

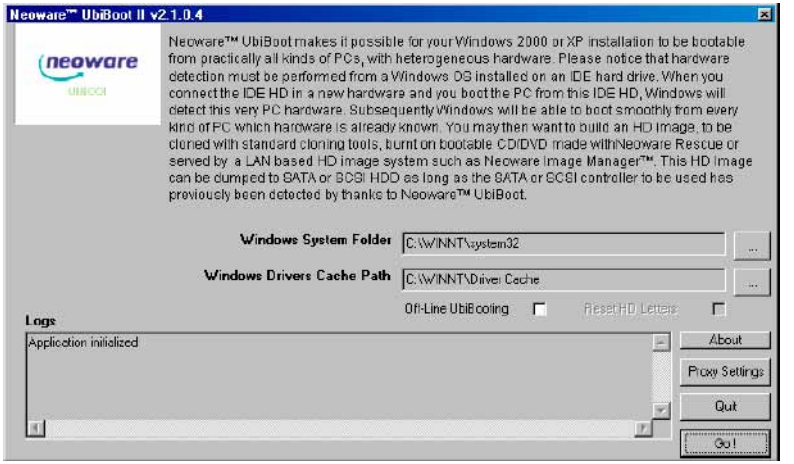
The following basic procedure describes how to create a Windows system hard disk that can boot a variety of PC hardware configurations. It assumes that you have already installed the **Client** components of Neoware Image Manager on a regular IDE hard disk containing a correctly configured Windows installation in partition **C:** (partition size should not exceed 10 GB), and an image of that partition has been created using Client Builder.

1. Boot a client device off an image containing Neoware UbiBoot. Note that the mode (Admin mode, Volatile mode, etc.) does not really matter as long as you run UbiBoot and then Active Cloner without rebooting between the two operations.
2. Log on as a user with Administrators Rights.
3. Run Neoware UbiBoot from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware UbiBoot**.



Note that you can also run the Neoware UbiBoot executable (`ubiboot.exe`) "directly", as long as all the required files (`QDrivers.QAR` and `license.txt`) are stored in the same directory.

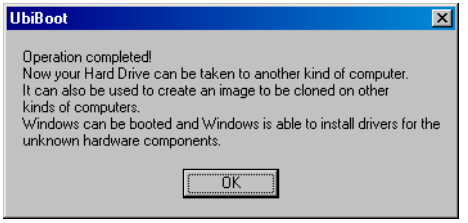
4. Check that the **Windows System Folder** path and **Windows Drivers Cache Path** are correct for the hard disk being UbiBoot'ed.


Neoware™ UbiBoot II v2.1.0.4
neoware
Neoware™ UbiBoot makes it possible for your Windows 2000 or XP installation to be bootable from practically all kinds of PCs, with heterogeneous hardware. Please notice that hardware detection must be performed from a Windows OS installed on an IDE hard drive. When you connect the IDE HD in a new hardware and you boot the PC from this IDE HD, Windows will detect this very PC hardware. Subsequently Windows will be able to boot smoothly from every kind of PC which hardware is already known. You may then want to build an HD image, to be cloned with standard cloning tools, burnt on bootable CD/DVD made withNeoware Rescue or served by a LAN based HD image system such as Neoware Image Manager™. This HD image can be dumped to SATA or SCSI HDD as long as the SATA or SCSI controller to be used has previously been detected by thanks to Neoware™ UbiBoot.
Windows System Folder
C:\WINNT\system32
Windows Drivers Cache Path
C:\WINNT\Driver Cache
Off-Line UbiBooting
Reset HD Letters
Logs
Application initialized
About
Proxy Settings
Quit
Go!

5 Click the **Go!** button.

6 An end-user License Agreement dialog will be displayed. Read the agreement and, if you agree to the terms, select **I accept** then click the **Go On** button.

UbiBoot will install and configure the required drivers. An **Operation Completed** message will appear when successful.


UbiBoot
Operation completed!
Now your Hard Drive can be taken to another kind of computer.
It can also be used to create an image to be cloned on other kinds of computers.
Windows can be booted and Windows is able to install drivers for the unknown hardware components.
OK

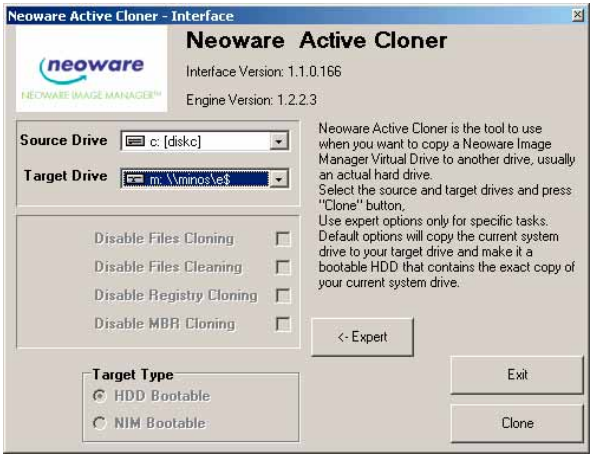
The virtual hard disk is now UbiBoot-enabled.

7 Run Neoware Active Cloner.

To run Neoware Active Cloner from the **Start** menu, select **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Active Cloner**.

Note that you can also run the executable file (`NIMCloner-GUI.exe`) “directly” as long as the required files (`NIM-Cloner.exe`, `NRdmpSvc.exe` and `VVSAToolsDll.dll`) are stored in the same directory as the executable file.

Select as the target the hard disk drive that you will be using to detect the new hardware whose support is to be added to the operating system on the virtual disk drive. Keep the default settings in Active Cloner.


Neoware Active Cloner - Interface
neoware
NEOWARE IMAGE MANAGER™
Neoware Active Cloner
Interface Version: 1.1.0.166
Engine Version: 1.2.2.3
Source Drive
c: [diskc]
Target Drive
m: \\minos\e$
Neoware Active Cloner is the tool to use when you want to copy a Neoware Image Manager Virtual Drive to another drive, usually an actual hard drive.
Select the source and target drives and press "Clone" button.
Use expert options only for specific tasks. Default options will copy the current system drive to your target drive and make it a bootable HDD that contains the exact copy of your current system drive.
Disable Files Cloning
Disable Files Cleaning
Disable Registry Cloning
Disable MBR Cloning
<- Expert
Target Type
HDD Bootable
NIM Bootable
Exit
Clone

The target HDD can be attached directly to the client (as a non-bootable drive). As an alternative, the target HDD root folder can be a shared folder, locally mounted on the client (Neoware Active Cloner needs a drive letter to access the target drive).

The target HDD must have been partitioned and formatted under Windows. Its main partition must be large enough to contain the content of the Virtual Disk Drive. Its main partition must have been activated.

Refer to the chapter “Neoware Active Cloner” on page 271 for more details.

8 When Active Cloner has completed, shutdown the computer that the target HDD is physically connected to (the client or the computer that is sharing the target HDD root folder). The target

HDD now has a UbiBoot-enabled Windows installation in its system partition.

9 Connect the target HDD to the platform whose hardware is to be detected in order to add support for it.

10 Switch on the PC or TC so that it boots off the target HDD. Windows will automatically detect the new hardware configuration and may ask you to provide driver media (CD-ROM) or reboot the PC or TC - do so when prompted.

If you experience any problems during this phase, please refer to the section “HAL Considerations” on page 113.

11 Apply any required patches, new drivers, or chipset utility.

12 Check in the Windows Device Manager that all the hardware has been installed successfully and is working correctly. (Right click on the **My Computer** icon, select **Properties**, click on the **Hardware** tab, then the **Device Manager** button.)

13 When all the hardware is working as expected, use Client Builder to create an image of the system partition. That image may now be used as a bootable virtual hard disk on any PC or TC of both hardware configurations.

If you need to add another hardware configuration, run UbiBoot in the newly created image and click **Go!** *before* cloning the virtual drive to the actual HDD. Then repeat steps 7 to 12.

14 Once all the required hardware has been recognized by the Windows configuration, it is recommended that the resulting virtual hard disk be defragmented.

15 This virtual hard disk is now bootable on all hardware configurations that have been used in steps 7 through 12. It may also be cloned onto a hard disk that may be used to boot Windows 2000/XP/XP Pro on those different hardware configurations (or the actual target HDD in its latest state can be used for this purpose).

A hard disk image is created by running Client Builder on any of the clients that can be booted from the target HDD, as described in the chapter "Creating a Client Image" on page 39. If in the future you need to add or change a client configuration in the hard disk image, you may need to transfer the image to an actual IDE hard disk to enable Windows to recognise the new client hardware configuration.

Using a UbiBoot Enabled Hard Disk

Learn to Use Unknown Hardware

You can make an instance of Windows 2000 or Windows XP learn to use unknown hardware. Use Neoware UbiBoot and then Neoware Active Cloner to create a UbiBoot-enabled hard disk drive, then connect that HDD to a PC or a TC containing the unknown hardware. Power-on the PC or TC and make it boot off the UbiBoot-enabled hard disk. Windows will detect the new hardware. You may need to provide drivers media (CD-Rom for instance) for the detected hardware. Windows may ask you to reboot the PC or TC and you should do so when asked to. In Device Manager, check that all the hardware has been successfully installed and is working according to your requirements. Once this is the case, the UbiBoot-enabled HD can be used to boot any client in which hardware has been detected and related drivers have been installed.

Master HD for Building Images

You can use a Neoware UbiBoot-enabled hard disk as a master HD for creating an image that can be used for cloning your systems. Make sure that the original master HD is an IDE hard disk. The following are IDE hard disks: UDMA 33, UDMA 66, UDMA 100, UDMA 133. SATA disk drives are also usually considered as IDE disk drives.

Detecting New Hardware

You must run Neoware UbiBoot each time you want to detect new hardware. If you don't run Neoware UbiBoot just before connecting the UbiBoot enabled HD to the new hardware, Windows may not be able to start correctly (BSOD, reboot…) and then it won't be able to detect the new hardware.

The correct procedure is as follows:

1. Connect the UbiBoot enabled HD to a client whose hardware is already known by the Windows installation stored on the virtual drive. We will call this client, Client-A and this HD, HD1.
2. Boot Client-A off the virtual drive.
3. Launch Neoware UbiBoot on Client-A.
4. Run Active Cloner and dump the virtual drive to HD1
5. Shutdown Client-A.
6. Remove HD1 from Client-A.
7. Connect HD1 to a client whose hardware is not already usable by the Windows installation stored on the virtual drive (we will call this client Client-B).
8. Boot Client-B off HD1. Let Windows detect the new hardware and provide drivers when you are asked to. Reboot Client-B each time you are asked to.
9. Make sure all the devices are correctly detected and that the drivers for them are running correctly (check this in Device Manager).
10. Apply any patches, new drivers or chipset utilities that you need to apply.

Now HD1 can be used to boot Client-A and Client-B, and any other clients that have the same hardware configuration. You can also boot Client-A or Client-B off HD1 and create a new image (virtual drive) with Client Builder.

Updating or Removing Drivers for Off-line Devices

You can update all the drivers for different clients on a single computer that boots a Neoware UbiBoot enabled system. You can also delete drivers for devices that will not be used anymore. In most cases you can perform the following procedure:

1. Right-click on **My Computer** and select **Properties**.
2. Click on the **Advanced** tab.
3. Click on **Environment Variables**.
4. Click on the **New** button near the bottom of the dialog, below the **System variables** list box.
5. For **Variable Name**, enter `devmgr_show_nonpresent_devices`.
6. For **Variable Value**, enter **1**.
7. Click **OK** to close **Environment Variables** and **OK** again to close **System Properties**.
8. Right-click on **My Computer** and select **Properties**.
9. Select **Manage**.
10. Click on **Device Manager**.
11. In the **View** menu select **Show hidden devices**.
12. Select the name of the device requiring the updated driver.
13. Right-click on the device and select **Update Driver**.
14. Provide the path to the driver file.

Occasionally this procedure may not work; the driver may not work as expected, or the update wizard does not work when Windows fails to detect the actual device. If this is the case, you should boot the PC containing the device whose driver is to be updated and update the driver in the usual way.

You can use this procedure if you want to delete existing drivers for devices that will not be used anymore; in step 13 choose to remove the device.

Additional Uses for Neoware UbiBoot

Creating a Windows Installation that can Run Unknown Hardware

Neoware UbiBoot enables you to create a Windows installation that can be run on unknown hardware. This can then be used as a hardware independent pre-installed and preconfigured Windows installation (containing Windows System and applications). The hardware will be detected and configured when Windows boots on each different hardware.

In order to achieve this, run Neoware UbiBoot and then run Active Cloner to dump the UbiBooted OS installation to an actual HDD. Use this actual HDD to create the Windows installation that will be able to boot unknown hardware. (For instance, use this HDD to create an image ready to be deployed using a cloning tool.)

Creating a Windows Installation that can Run Heterogeneous Hardware

You can boot a Neoware UbiBooted system disk on each of the PC hardware configurations being used so that Windows recognises them and loads the required drivers. Then you can use this Windows installation to build a master image for deployment with cloning tools, or build a disk image for use with Neoware Image Manager or CD/DVD-Boot systems.

HAL Considerations

HAL (Hardware Abstraction Layer) is the Windows component that controls communications between the operating system and the hardware. There are several types of `HAL.DLL` file and the one used depends on the hardware Windows is installed on:

- *Standard PC HAL*, Non-ACPI PIC (`HAL.DLL`)
- *MPS Uniprocessor PC HAL*, Non-ACPI APIC UP (`HAL-APIC.DLL`)
- *MPS Multiprocessor PC HAL*, Non-ACPI APIC MP (`HALMPS.DLL`)

- *Advanced Configuration and Power Interface (ACPI) PC HAL*, ACPI PIC (`HALACPI.DLL`)
- *ACPI Uniprocessor PC HAL*, ACPI APIC UP (`HALAACPI.DLL`)
- *ACPI Multiprocessor PC HAL*, ACPI APIC MP (`HALMACPI.DLL`)

Usually there is an ascending compatibility between HALs. For instance, *Standard PC HAL* is the most compatible HAL. If your Windows installation uses *Standard PC HAL*, when it is UbiBoot-enabled it should be able to boot ACPI computers etc., but you won't be able to use ACPI-specific functions (such as ACPI power button functions).

On the other hand, if your Windows installation uses *ACPI Uniprocessor PC HAL*, this instance of Windows will not be able to boot Standard PCs (non-ACPI) or "ACPI only" computers, even after it has been UbiBoot-enabled.

When you want to deploy a UbiBoot-enabled Windows installation to clients that could use different HALs, you must make sure that Windows installs the most compatible HAL. The best practice is usually to build the reference Windows installation using the oldest computer in your fleet, or to use a "Standard PC" Windows setup (press the **F5** key during the first part of Windows installation, then when you can see **Press F6 if you need to install a SCSI or RAID controller**, select **Standard PC** as the PC type for your Windows installation).

Note that Neoware thin clients are compatible only with *Standard PC HAL*, Non-ACPI PIC (`HAL.DLL`) and *Advanced Configuration and Power Interface (ACPI) PC HAL*, ACPI PIC (`HALACPI.DLL`).

Mixing ACPI & Non-ACPI Computers

Advanced Control and Power Interface (ACPI) is considered by Windows 2000/XP/2003 OS as the root-most device in a PC architecture. A Windows 2000/XP/2003 installation that was made for an ACPI enabled computer will not be able to boot a non-ACPI computer, even if Neoware UbiBoot has been applied to the system HD. In case you have to mix ACPI and non ACPI computers that must boot from the same HD (or HD image, cloned HD etc), you must perform your original Windows® 2000/XP/2003 installation on a non ACPI computer, or downgrade your HAL.

Mixing Unicore & Multicore (or multi-CPUs) Computers

The HAL to use in order to take advantage of multi-CPUs (or multicore CPUs) is the *ACPI Multiprocessor PC HAL*, ACPI APIC MP (`HALMACPI.DLL`). Note that this HAL cannot be used on Unicore CPU computers. The Unicore capable HALs can be used to boot Multicore computers, but in this case only one core is used. This is not recommended for performance reasons. If you have to manage a fleet of computers that comprise Unicore and Multicore computers, it is recommended that you create several different images with the appropriate HALs.

HAL Selection

Choosing a Specific HAL at Windows Installation

You can specify the HAL to use when performing the Windows installation. If the Standard PC HAL is chosen, Windows will be installed with APM (Advanced Power Management) support, not ACPI. APM is the predecessor of ACPI.

If you perform Windows installation on a non-ACPI compatible PC, Windows will generally be installed with Standard PC HAL. If you don't have a non-ACPI PC when you perform your installation of

Windows, you can disable ACPI in your PC BIOS setup before you install Windows.

You can also press the **F5** key during the first part of the Windows installation (when you can see **Press F6 if you need to install a SCSI or RAID controller**). Then select **Standard PC** as the PC type for your Windows installation, or the specific HAL you want to use.

Note: *Non-ACPI installations of Windows can boot ACPI computers. The opposite is not true. When a computer does not use ACPI, it can't use advanced power control features such as hibernation, stand by, software shutdown when the power button is pressed, etc.*

Downgrading HAL After Windows Installation

You can use an existing Windows installation and "downgrade" the HAL used by Windows. The procedure is as follows:

1. Open the Device Manager (**Control Panel** > **System** > **Hardware** > **Device Manager**).
2. Develop the entry under **Computer**.
3. Right-click on this entry.
4. Select **Properties**.
5. Click the **Driver** tab.
6. Click the **Update Driver** button.
7. Select **Install from a list or specific location (Advanced)**, then click **Next**.
8. Select **Don't Search, I will choose the driver to install**, then click **Next**.
9. Make sure the **Show compatible hardware** check box is checked.
10. Select the desired HAL, then click **Next**.

    Note that if you plan to boot a Neoware thin client off the image you are currently modifying, you must select either ***Standard PC*** or ***Advanced Configuration and Power Interface PC***.

11 Click **Finish** then **Close**.

12 Reboot the computer.

13 Let Windows re-detect the hardware (detection may not occur).

The HAL used by the Windows installation on the system drive (either HDD or virtual drive) is now the one you just selected.

Recommended HAL

Depending on the fleet of computers that must boot off the same UbiBooted drive, we recommend you use the following HAL:

- If all your clients are ACPI compatible, our recommendation is to use **Advanced Configuration and Power Interface (ACPI) PC HAL** (original file name `HALACPI.DLL`).
- If you have at least one type of client that is not ACPI compatible, our recommendation is to use **Standard PC HAL** (original file name `HAL.DLL`).

HAL Related Resources

The following Internet links are useful for obtaining more information about HALs.

- HAL options after Windows XP or Windows Server 2003 setup:
  `http://support.microsoft.com/?kbid=309283`
- How to force a HAL during an upgrade or an installation of Windows XP:
  `http://support.microsoft.com/default.aspx?scid=kb;EN-US;299340`
- How to troubleshoot Windows 2000 HAL issues:
  `http://support.microsoft.com/default.aspx?kbid=237556`
- How to determine the HAL that is used in Windows XP:
  `http://support.microsoft.com/?kbid=298898`

Windows Product Activation

When changing the hardware of a Windows system that needs to be activated (Windows XP, Microsoft Office XP, etc.), you may need to re-activate the product.

It is recommended that you use VLA (Volume License Agreement) editions of the products. VLA editions do not need to be activated. If VLA editions are not available, you may have to enter each PC's own product serial key in order to re-activate. This may also require that you use the "activation by telephone" feature.

Check the following Internet links for more details about Activation:

`http://www.microsoft.com/windowsxp/evaluation/features/activation.mspx`

`http://www.microsoft.com/piracy/activation_faq.mspx`

`http://support.microsoft.com/default.aspx?scid=kb;en-us;328874`

UbiBoot & Microsoft SysPrep

Neoware UbiBoot and Neoware Image Manager can be used in conjunction with Microsoft SysPrep. In particular, a Windows installation stored on a virtual drive can be resealed using SysPrep's "Reseal" feature before it is deployed. This can be useful especially if your clients will be using Normal mode.

With Neoware UbiBoot, the administrator just lets Windows 2000/XP/2003 learn to detect and use the hardware. With Microsoft SysPrep used to build a Windows installation that can boot heterogeneous hardware platforms, the administrator needs to take inventory of all the hardware components and identify and copy the driver files for all these components.

Neoware UbiBoot builds a single image integrating all drivers. Microsoft SysPrep does not create a single image containing all drivers; the driver integration process must be repeated each time

after the image is enriched with new or modified hardware, necessitating the handling of multiple logical images.

Note that both Neoware UbiBoot and Microsoft SysPrep may be used together. SysPrep will not overwrite what UbiBoot has done.

UbiBoot Expiry Date

The UbiBoot expiry date, if any, only affects the GUI application that runs when you apply Neoware UbiBoot. It has no effect on the Windows installations you have created using UbiBoot.

Troubleshooting

I get a "Security Check Failed" error when running Neoware UbiBoot.

Some versions of Neoware UbiBoot check that the product has not expired by getting the current time from the Internet. This message may be displayed if it cannot access the Internet to check the time, or if your copy of Neoware UbiBoot has expired. In that case, please contact your Neoware representative for a renewed license.

I get a "Cannot perform security check. Please make sure your computer is connected to the Internet" error when running Neoware UbiBoot.

Neoware UbiBoot uses HTTP and then SNTP protocol to get the current time from the Internet. The PC that runs Neoware UbiBoot must be able to act as an HTTP client or a SNTP client. If you cannot get the time from the Internet, you must check the following:

- Your client is actually connected to the Internet or can do "Web Browsing" using port 80, either directly or through a proxy. You can specify the proxy settings by clicking the **Proxy Settings** button in the Neoware UbiBoot dialog**.**

- Your client can use at least one of the following protocols:

  HTTP protocol using port 80, either directly or through a proxy server.

  SNTP protocol to connect to NTP servers outside your LAN. This protocol uses UDP port 123. If you are behind a network address translator, you may need to configure your network address translator ports redirection for this purpose.

I applied Neoware UbiBoot to a Windows installation and cloned it to an actual HD, but the HD cannot boot my new client.

You must run Neoware UbiBoot on a well-known computer (a computer whose hardware is totally known by Windows) ***just before*** moving the HD to the new computer.

Boot a well-known computer with the Windows installation on your virtual drive. Then run Neoware UbiBoot on this client. Clone the virtual drive to the actual HDD using Neoware Active Cloner. Shutdown the client, remove the HDD and connect it in the new client. Note that if the Windows installation was made with ACPI capabilities or HAL specific capabilities, the new client must have the same capabilities. (See also the section “HAL Considerations” on page 113.)

When a Windows installation used on Client-A cannot boot Client-B even after this Windows installation has been UbiBoot enabled, it is recommended that you install and run UbiBoot on the Windows installation that can boot Client-B, and use this on Client-A.

If you have performed off-line UbiBooting, you may apply UbiBoot on the off-line system again and make sure you selected the **Reset Drive Letters** option.

After I applied Neoware UbiBoot successfully, Windows detected my new hardware and is running correctly but is very slow and reacts as if it was overloaded.

There might be a process that is using a lot of system resources. Open the Task Manager, click on the **Process** tab, check the box **Show processes from all users**, sort the process by CPU occupation and check if there is a process other than System Idle Process that is using the CPU intensively. If so, kill this process and check that Windows is running better. If this is the case, you will need to make sure that this process is not launched at Windows start time. You may need to uninstall some applications, disable some services, delete entries in the **Startup** folder of the **Start** menu, or delete some entries in the registry keys that control automatic startup of applications.

After moving a UbiBooted HDD that was made for an Intel-based Windows installation to an AMD-based computer, the AMD-based computer cannot boot. The computer blue screens, freezes or reboots during boot process.

This is usually caused by `IntelPPM.SYS` driver that cannot run on AMD based computers. To rectify this, disable `IntelPPM.SYS` before cloning the virtual drive. This does not usually cause any problem on the Intel or AMD based computer.

To disable `IntelPPM.SYS` you can use the following Registry file and merge it into Windows registry before cloning the virtual drive to the actual HDD:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Ser-
vices\IntelPPM]

"Start"=dword:00000004
```

After moving an UbiBooted HDD that was made for an AMD-based Windows installation to an Intel-based computer, the Intel-based computer cannot boot. The computer blue screens or reboots just before the desktop should be displayed.

This is caused by AMD specific utilities that cannot run on Intel based computers. To rectify this, uninstall (or don't install) any AMD specific utility before cloning the virtual drive to the actual HDD.

CHAPTER 10

Managing Local Hard Disk Access

This chapter describes how to enable or disable client access to local hard disks.

Introduction

Neoware Image Manager clients can be customized in order to enable or disable access to local hard disks. This is achieved using the Local HD Manager wizard `LocalHDManager.exe`.

The Local HD Manager wizard modifies a virtual disk image so that client local hard disks can be made available or unavailable, and enable new local HDs to be accessed (that is local hard disks that have never been detected nor used by the Windows instance currently running) without rebooting the clients. This is very useful when the volume write mode is set to volatile.

Local HD Manager should be run only on diskless clients. When run on clients booted off actual HDs, if local HD access is disabled, Windows won't be able to access the local HDs after a reboot and then won't be able to complete the boot process.

Using the Local HD Manager

Once the client computers boot correctly with Neoware Image Manager, use Local HD Manager as follows:

1 Shutdown all the clients.

2 Backup the HD image on the server.

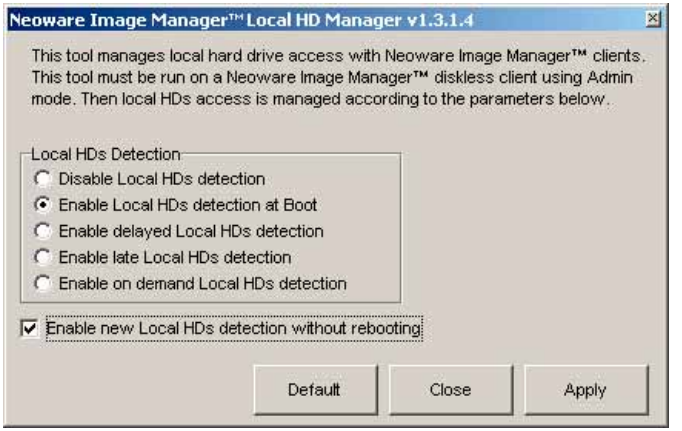
3 Modify the relevant `nvdd` configuration (using Neoware Image Manager Console or a text editor) so that the virtual volume will be opened in Admin mode.

4 Reload the new configuration to the NVDD server module (either click the **Reload conf file** button in the Neoware Image Manager Console **NVDD Manager** dialog, or stop then restart the NVDD server module).

5 Boot ONE client.

6 Log on this client using an *Administrator Account*. (A user account with administrative rights. This account can be a local user account or domain user account, as long as it has complete control over the client computer.)

7 On this client, run Local HD Manager from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Local HD Manager**, or by executing the file `LocalHD.exe`.


Neoware Image Manager™ Local HD Manager v1.3.1.4
This tool manages local hard drive access with Neoware Image Manager™ clients. This tool must be run on a Neoware Image Manager™ diskless client using Admin mode. Then local HDs access is managed according to the parameters below.
Local HDs Detection
Disable Local HDs detection
Enable Local HDs detection at Boot
Enable delayed Local HDs detection
Enable late Local HDs detection
Enable on demand Local HDs detection
Enable new Local HDs detection without rebooting
Default
Close
Apply

8 Select the required parameters then click the **Apply** button.

Typical settings are:

Disable Local HDs detection - Windows will not be able to access local disk drives.

Enable delayed (or late) local HDs detection - Windows will detect the local disk drives in the second (or third) part of the boot process (not as boot devices). This is useful when there are issues accessing certain local disk drives.

The option **Enable new Local HDs detection without rebooting** must be selected if you want your user to be able to access "unknown" local disks without having to reboot the client computer which, if the system volume is mounted in Volatile mode, will have to keep rebooting in order to access the local drives.

Note: *This option may need to be set again after some unknown local disk has been detected when the system volume was mounted in non-volatile mode. Actually, when Windows detects a new hard drive, it restores the default behaviour for Windows, which corresponds to the Local HD Manager parameters* ***Enable Local HD detection at boot*** *and* ***Disable new Local HD detection without rebooting****.*

Clicking the **Default** button then the **Apply** button will set the client operating system so that it behaves as if Local HD Manager had never been used. Local disk drives will be detected at boot time, and a reboot will be required to be able to use unknown HDs.

9 Read the warning messages (if any) and click the appropriate buttons.

10 Close the Local HD Manager by clicking the **Close** button.

11 Shutdown Windows.

12 Modify the relevant `nvdd` configuration (using Neoware Image Manager Console or a text editor) so that the virtual volume will be opened in the previous mode (usually Volatile mode).

13 Reload the new configuration to the NVDD server module (either click the **Reload conf file** button in the Neoware Image Manager Console **NVDD Manager** dialog, or stop then restart the NVDD server module).

14 Start at least one client computer and check that access to the local HDs meet your requirements.

NOTES

- Note that the **Local HDs Detection** setting will apply to all local HDs. If you need more detailed options, such as preventing some specific drive letters to appear in Windows Explorer, you may want to use TweakUI. This free tool can be download from the following link:
  `http://www.microsoft.com/ntworkstation/downloads/PowerToys/Networking/NTTweakUI.asp`
- When a new hard drive is detected while the HD image is not mounted in Volatile mode, you may need to run Local HD Manager again. Actually, when Windows detects a new hard drive, it restores the default behavior for Windows, which corresponds to the Local HD Manager parameters **Enable Local HD Detection at boot** and **Disable new local HD detection without rebooting**.

CHAPTER 11

Windows Product Activation

This chapter describes how to activate Windows products for Image Manager clients.

Introduction

Windows XP and some other products edited by Microsoft need to be activated. This activation is made through a link between a unique Product Key and data that are specific to each computer. When you are using client stations that are based on 100% identical hardware, it is theoretically possible to activate the product only once (for one station) and to use this product on other client stations, for instance when using HD cloning products.

For example, it is theoretically possible to activate all the products that need to be activated before building the HD image with Neoware Client Builder. However, it may be illegal to use Microsoft products this way, even if there are legal licenses for all the products and all the client stations.

If you want to use Microsoft products this way (single activation for several clients), you must contact your Microsoft representative. If you want to use Microsoft products that need to be activated on several client stations, it is recommended that you use the *Volume License* edition of the products. Volume License products do not need to be activated individually.

It is possible to activate the products individually, even when the HD image is shared among several client machines. You may use

CVolwrite/Persistent (or CVolwrite/Normal) client writing mode so that each client machine would have its own activation link.

Product Activation Procedure

The administrator can use the following procedure to activate products.

1. Modify the `nvdd` configuration file (using Neoware Image Manager Console or a text editor) so that the system volume will be opened in CVolwrite/Persistent write mode (or in CVolwrite/Normal mode).
2. Reload the new configuration to the NVDD server module (either click the **Reload conf file** button in the Neoware Image Manager Console **NVDD Manager** dialog, or stop then restart the NVDD server module).
3. Boot all the clients and activate them individually. Of course, you must follow the procedures that allow a specific Product Key to be entered for each client station. For details, refer to the following articles:

   `http://support.microsoft.com/?kbid=810892`

   `http://support.microsoft.com/default.aspx?scid=kb;en-us;Q328874`

   `http://xphelpandsupport.mvps.org/how_do_i_change_the_windows_xp_p.htm`
4. If you use CVolwrite/Persistent mode, once all the activations are done, reboot the clients so that the reference CVol files are created.
5. You may then change the system volume opening mode to a mode in which the CVol files are retained after clients reboot, as long as you keep the reference CVol files in order to be able to restore the activation link in case it has been lost or destroyed. The best client writing mode to use is CVolwrite/Persistent mode (or CVolwrite/Normal mode if it is required that modifications to the system volume are kept after a reboot).

When you use this method to manage activations, you must re-activate each client computer every time the shared HD image file is modified. This is because the reference CVol files that contain the individual activation data are not valid anymore (they contain client-specific differences (deltas) to the HD image file).

CHAPTER 12

Windows User Profiles

This chapter describes how to configure your Neoware Image Manager system so that clients can use Windows user profiles.

Domain Roaming Profiles

Neoware Image Manager can be used to set up a system in which user profiles are kept persistent. This is a “thin client like” usage.

In order to do so, you can use a standard Windows Profiles system, using a logon server (Windows NT Server, 2000 Server or Samba Server), domain logon and profile paths.

Note that if your client OS is Windows XP SP1 (or later) and your profiles are stored on a Samba server, you may need to enable the policy **Do not check for user ownership of Roaming Profile Folders**. To do this, run `gpedit.msc` and go to **Computer Configuration** > **Administrative Templates** > **System** > **User Profiles**.

Windows Roaming Profiles are copied from the Profiles server to the "local disk drive". You should keep the profile files as small as possible. In particular, the administrator should use folder redirections for `My Documents` folders and other folders that are, by default, embedded within the profile.

"Local" Roaming Profiles

You can use an original setup where all the users are created only on the reference local shared configuration (in fact in the local system users accounts database). Users are created on a client computer booted from an actual HD or from a remote HD Image in Admin mode. Here are some tips for this kind of setup:

1. Create the required user accounts on the Windows XP/2000 client reference installation. These accounts are local to the Windows 2K/XP Reference configuration (not domain or Active Directory users accounts). The accounts can either be created on a local HD that will later be used as a reference for a virtual volume image file, or they can be created directly on the virtual volume when the NVDD server module is configured so that the virtual volume is opened in Admin mode.
2. Identify a computer that will host Profiles for the users. This will now be referred to as the Profile server.
3. On the Profile server, create one account per user created in step 1, and also create one shared folder per user created in step 1. Account names must be the same as the user names created in step 1. Apply access rights so that each user has read-write access to their own shared folder. In each user shared folder, create a sub folder named `PROFILE`.
4. Make sure the folders `\\<ProfileServerIPAddressOrName>\<UserName>\PROFILE` exist and are accessible. Each user must have total control (Read/Write/Execute) in their profile folder.
5. Modify the `nvdd` configuration (using Neoware Image Manager Console or a text editor) so that the volume in which you want to add the user accounts will be opened in Admin mode.
6. Reload the new configuration to the NVDD server module (either click the **Reload conf file** button in the Neoware Image Manager Console **NVDD Manager** dialog, or stop then restart the NVDD server module).

7. Boot only ONE client.
8. On the client computer, issue the following command at the command prompt for each user created earlier:

   ```
   net user <UserName> /profilepath:\\<ProfileServerIP-AddressOrName>\<UserName>\PROFILE
   ```

9. Log on successively with each user login name and password and check that everything is running correctly. (This step is recommended because it will create the appropriate "local profile folders" for every user.)
10. Shutdown the client station.
11. Restart the server so that it shares the virtual drive in CVolwrite/Normal mode, or in CVolwrite/Volatile mode.
12. Start any of your Neoware Image Manager client computers and log on with any of the user names and passwords used in step 9.
13. Log off this user.
14. On another Neoware Image Manager client station, log on with the user name and password used in step 12. Check that the profile (desktop, shortcuts, bookmarks/favorites) is the same.

Using this user management method, the users accounts database is stored in a virtual drive that can be opened in Admin mode to make any desired changes. This user management method relies only on the "reference" Windows system local user database.

TIP

Some settings can be fine-tuned in the users profiles:

In the registry, in the key:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
```

the value `ExcludedProfileDirs` (string) can be tuned. This value is a list of folders that do not get copied from central profile mounting point to local profile (refer to *Profile* sections in Windows Network-

ing documentation). Local Settings may contain, typically, Outlook files, WallPaper etc.

The directories `Local Settings` and `History` should not be in this list. The directory `Local Settings\Application Data\Microsoft\Windows` may be in this list, though it is not in this list by default.

This setting can be applied to `HKEY_USERS\.Default` before the users are created. Then, this setting does not need to be applied individually for all users after they have been created.

Related resources:

`http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/maintain/XPUsrDat.asp`

Folders Redirection

When using Roaming Users Profiles, whether Domain based or "Locally" based, you should redirect each user's `My Document` folder outside the profile itself, and also redirect the folder where user's email data is stored. Please refer to the following documents for more details:

`http://support.microsoft.com/kb/232692`

`http://www.microsoft.com/technet/community/newsgroups/upfrfaq.mspx#XSLTsection122121120120`

`http://technet.microsoft.com/en-us/library/bb490855.aspx#EIAA`

Redirecting these folders is very useful in order to reduce the users' profiles size. Each roaming profile is copied "locally" on the client local volumes when the user logs on, so large profiles lead to longer logon time (when Windows displays **Loading Your Personal Settings**), stressed networks and long logout times (when Windows displays **Saving Your Personal Parameters**).

CHAPTER 13

Adding Clients & New Software

This chapter describes how to add a new client, add new software, and restore a virtual hard disk volume to an actual hard disk.

Adding a New Client

When you add a new client so that it boots off one of the existing virtual drives, its hardware must be 100% identical to the clients that can boot off that virtual drive. In particular, the network card must be in the same PCI slot for both clients. If this is *not* the case, please refer to the UbiBoot sections in the chapters "Building a Virtual Hard Disk to Boot any PC or TC" on page 103, and "Adding Network Boot Devices to an Image" on page 87.

To add a new client with identical hardware:

1. Make sure that the new client is able to get an IP address from the DHCP server.
2. Boot the new client.

Repeat this process to add more clients.

Note: *You can use clients that have different hardware as long as the reference hard drive can boot each hardware configuration. Hard drives that have been enhanced using Neoware UbiBoot and that have been used to boot and perform automatic hardware detection can be used to build HD images usable by clients with different hardware, after each hardware configuration has been recognized by the Windows installation on the HD.*

Modifying an HD Image to be Used by Several Clients

Using Admin Mode

The following procedure enables you to make changes to a hard disk image that is used by several clients. For example, to add a new application so that it is available to all the clients. This must be done each time you want to modify the reference configuration so that every client can benefit from the changes you make.

Note: *This is the method that you will use every time you want to make changes to the system drive, such as adding a new application, but also applying system and software patches, modifying the system configuration, modify some registry settings, adding users, etc. The changes that are performed this way will be applied to every station that uses the modified volume when it is shared.*

1. Shutdown all the clients connected to the volumes that will be affected by the installation of the new application (e.g. the system volume and, potentially, other volumes that will store some of the files that are part of the new application).

   In order to update a volume currently used by clients, you may also copy the HD image file you want to modify and configure Neoware Image Manager so that the client used to perform the changes will mount the copy of the HD image file in Admin mode. This client will then be the only client that mounts the volume in Admin mode, making it possible for the clients currently using the original HD image file to keep on working. You can copy a hard disk image file that is currently being used by clients, as long as it is not opened in Admin mode. We recommend that you check that this copy will not decrease server performance.

2. Modify the `nvdd` configuration (using Neoware Image Manager Console or a text editor) so that the virtual volume on which the changes are to be made is served in Admin mode to the client that will perform the changes.

3. Reload the new configuration to the NVDD server module (either click the **Reload conf file** button in the Neoware Image Manager Console **NVDD Manager** dialog, or stop then restart the NVDD server module).
4. Boot only the client that will perform the changes.
5. Log on to this client with a user that has enough rights to perform the desired changes on the volume.
6. Install the new application(s), patches, and modify the configuration. You can reboot as many time as you want.
7. Once the reference configuration suits your requirements, shutdown the client.
8. Modify the `nvdd` configuration so that the virtual volume on which the changes are to be made is served to the desired clients in the desired mode (usually CVolwrite/Volatile).
9. Boot all your clients. Now they all can use the new application, the new system settings are applied to them, etc.

Using the CVolMerge Tool

When you use CVolwrite/Normal mode, it is possible install applications and make changes to the system volumes that survive a reboot of the client computer. However, these changes are available only to the actual client computer on which they have been made. When you want to make a HD configuration that is currently only available to a specific client to be a new common virtual volume, you can use the `CVolMerge` tool. This tool builds a new HD image from a server based CVol write cache file and the corresponding HD image file. This new HD image file is equivalent to the logical volume composed by the client CVol file, plus the former HD image file.

The following procedure will enable you to add a new application that will be available to all the clients. For more details on the `CVolMerge` tool and how to reduce the size of a CVol file using the `CVolCompactor` tool, refer to the chapter “Merging Image & CVol Files” on page 177.

1. Make sure your NVDD server module runs so that the system volume you want to modify is mounted in CVolwrite/Normal mode by the client used to perform the changes on the HD image file. Let us assume that the volume you want to modify is named `MyDisk` and that the corresponding image file path is `/HDImages/MyDisk.vol`. Let's also assume that the CVol files for this volume are stored in `/CVols` on your server. You can, for example, make sure that the client that will be used to perform the changes is listed in the Normal clients in the **Volume Properties** dialog **Parameters** tab.
2. Boot one client. Let's assume this client has the MAC address 00-e0-c5-59-32-ed. The other clients can be up and running during all this process.
3. Log on to this client as a user that has enough rights to install applications. Install the new application(s), patches, and modify the configuration as required. You can reboot as many time as you need to.
4. Once the reference configuration suits your requirements, shutdown the client.
5. Locate the file `CVolMerge` (or `CVolMerge.exe`) in the Neoware Image Manager Distribution software (usually in `SERVER/LINUX/TOOLS` or `SERVER\WINDOWS\TOOLS` folder). Copy this file on your server HD. Let's assume this copy of the CVolMerge file is `/Tools/CVolMerge`.
6. Open a command prompt to your server and if required log on as a user that has administrative rights to the server.
7. At this command prompt, launch the file `CVolMerge` as follows:

   ```
   /Tools/CVolMerge /HDFiles/MyDisk.vol /CVols/
   MyDisk@00E0C55932ED /HDFiles/MyNewDisk.vol
   ```

   Note: *You must replace the paths to the files by the actual paths for the corresponding files in your server.*

   The CVolMerge tool displays its progression (in percentage).

8 When CVolMerge completes, you have two images: the original unchanged image on which clients are still running, and the new updated image. To make your clients boot from the new image, you can either (1) stop all clients and change the configuration file so that they boot from the new one, or (2) let the clients run the old image and make the NVDD server give them the new one the next time they reboot. These methods are as follows:

First Method:

1. Shutdown all the clients running the image.

2. Change the `nvdd` configuration so that the actual disk image file is changed from its old value (`/HDFiles/MyDisk.vol`) to its new value: `/HDFiles/MyNewDisk.vol`

OR

Stop the NVDD server module.

Rename the file `/HDFiles/MyDisk.vol` to: `/HDFiles/MyDisk.vol.bak`

Rename (or copy) the file `/HDFiles/MyNewDisk.vol` to: `/HDFiles/MyDisk.vol`

Second Method:

1. Change the configuration file and add the new volume. You can copy all the parameters of the unchanged volume to create this new one. Only the filename, and optionally the description, will change. In particular, the geometry parameters will remain the same.

2. When the new volume is included in the configuration file, make the clients boot from it. With this method, the running clients can continue their work. They will get the new image only when they reboot.

3. When you are sure that no clients are running on the old image, remove that image from the configuration file.

You can keep the old image definition in the configuration file. Then, when you update the new image using the CVolMerge tool, you can commit the changes to update the old image file which will become your newest image.

For example, let us assume you have two image files: `MyImage1.vol` and `MyImage2.vol`, and the corresponding volumes in the configuration file (`MyImage1` and `MyImage2`). `MyImage1` is your current production image. When you update it, you must commit the changes into the file `MyImage2.vol`. Then you configure the clients to boot off `MyImage2`. Later, when you want to update `MyImage2` (which is now your production image), you commit the changes to `MyImage1.vol` and set the clients to boot off `MyImage1`. Using this method is very efficient and secure, as you always have a backup copy of the unmodified image.

9 Start or reload the NVDD server module with its new configuration.

Now when the clients boot, they can use the new application, the new system settings are applied to them, etc.

Managing & Updating Images Located at Multiple Remote Sites

Neoware Image Manager servers are usually located on the same LAN as the clients that mount the virtual volumes. If you have several servers at different locations (at different branches for example), you may require a mirrored copy of the same image at each location. In this case the original mirrored copies of the image can be created at each location using a DVD-based or HD-based copy of the original Master image.

When an administrator wants to update an image that is mirrored on multiple remote Image Manager servers, it is not usually convenient to copy the complete updated image to each remote site over WAN. A more efficient way of updating remote images can be achieved by using scripts to activate the various image management tools that Neoware Image Manager provides. In particular, the tool `nvddadmin` can be used. Refer to the chapter "NVDD Server Administration" on page 241 for details.

The functions performed by the scripts could be as follows:

On the Master server (the server based at the Administrator facilities that contains the Master copy of the image):

1. Configure the NVDD server so that the image to be updated will be mounted in CVolwrite/Normal mode by the client to be used to update the image (Client-A).
2. Boot Client-A off the image and update it (run security patches, hotfixes, install or remove applications, change settings, etc.).
3. When the image works on Client-A as required, shut down Client-A.
4. Run `CVolCompactor` to reduce the size of the CVol file.
5. Compress the CVol file (using gzip, WinZip, etc.).
6. Copy the compressed CVol file to each of the remote NVDD servers containing the same image to be updated. (You can use the `nvddadmin` tool to do this.)

On the Remote NVDD server(s) (the server(s) containing the mirrored copy of the same image that is mounted by local clients):

7 Decompress (unzip) the CVol file. (You can use the `nvddadmin` tool to do this.)

8 Use `CVolMerge` to merge the CVol file and the image file into a new updated image file. (The `nvddadmin` tool can remotely launch `CVolMerge` on the remote server. `CVolMerge` will actually run on the remote server.

9 Change the `nvdd` configuration in order to serve the new image file to the clients. (The `nvddadmin` tool can retrieve the configuration file from the remote server and copy a new configuration to the remote server.)

The following is an example script that could be used on a Master server running Windows.

Note: *The following scripts have been provided as examples only, to illustrate the steps you need to perform in order to manage disk image mirroring. We cannot guarantee that the scripts will actually work or are free of errors.*

```
Rem  This script will copy a CVol file on a server
Rem  (accessed by its IP address or name) and create
Rem  a batch file that will create an updated image on
Rem  the remote server.

Rem  The CVol file to be sent to the remote server is
Rem  reduced in size using CVolCompactor, then the gzip
Rem  file compression utility is used to compress the
Rem  CVol file before copying it to the remote server.

Rem  This script assumes that gzip and the server tools
Rem  CVolMerge and CVolCompactor are in the PATH of
Rem  both servers.

Rem  %1 is path and name of the CVol header file (The
Rem  CVol Data file is then %1.dat).

Rem  %2 is the path of the folder that contains the Image
```

```
Rem  file on the Master server.

Rem  %3 is the image filename on the servers.

Rem  %4 is the UNC Path of the remote server folder in
Rem  which the CVol File is to be copied and where the
Rem  Image to be modified resides.


CVolCompactor %1 %2\%3 New%1
gzip New%1
gzip New%1.dat
copy New%1.gz %4 /y
copy New%1.dat.gz %4 /y

echo gzip –d New%1.gz > %4\RemoteJob.bat
echo gzip –d New%1.dat.gz >> %4\RemoteJob.bat
echo move New%1 %1 >> %4\RemoteJob.bat
echo move New%1.dat %1.dat >> %4\RemoteJob.bat
echo CVolMerge %3 %1 New%3 >> %4\RemoteJob.bat
echo Net stop nvdd >> %4\RemoteJob.bat
echo If exist Old%3 del Old%3 /y  >> %4\RemoteJob.bat
echo Ren %3 Old%3 >> %4\RemoteJob.bat
echo Ren New%3 %3 >> %4\RemoteJob.bat
echo Net start nvdd >> %4\RemoteJob.bat
```

The script `RemoteJob.bat` can now be run automatically. Its execution can, for example, be scheduled automatically by Task Scheduler with a simple script:

```
if exist <Path_to_file>\RemoteJob.bat call RemoteJob.bat
```

Restoring a Virtual Volume to an Actual Hard Disk

It may sometimes be necessary to dump the current system volume that a Neoware Image Manager client used to boot from to an actual hard disk. This is necessary if you intend to use Neoware UbiBoot in order for an existing volume to be used on new hardware and you cannot use the UbiBoot Extractor and Inserter tools. The "new hardware detection" enabled by Neoware UbiBoot can only be performed when Windows is run off an actual IDE or SATA hard disk. Some changes on network components, such as binding new service or protocols to a network interface in a client computer can also only be performed when Windows is run from an actual HDD.

To restore a system virtual volume onto an actual hard disk, you must use the Neoware Active Cloner tool. This tool can copy the current system volume to an existing partition in an actual hard drive.

Neoware Active Cloner can either be launched from a command prompt, as described here, or via a graphical user interface which is described in the chapter “Neoware Active Cloner” on page 271.

The procedure is as follows:

1. Connect an actual hard drive in the client that will be used to perform the operations (you can also connect this actual hard drive to another Windows computer in your local network).
2. Boot the client off the Neoware Image Manager volume to be cloned.
3. Log on to the client as a user that has administrative privileges.
4. If necessary, create a primary partition in the actual hard drive large enough to store the files in the current system partition. Mark this partition as Active (bootable). Use the computer to which the actual HD is physically connected to perform these operations.
5. If necessary, format the primary partition in the local HD using any of the filesystems supported by Windows. The filesystem of

the primary partition in the local hard drive can be different from the filesystem of the current system volume (for instance, the system volume can use FAT32 filesystem and the target partition can be formatted with NTFS filesystem). Use the computer to which the actual HD is physically connected to perform these operations.

6 Stop as many processes as possible on the Neoware Image Manager client. In particular, try to exit or stop all the processes that display an icon near the Windows clock and that have a **Stop**, **Exit** or **Quit** option. This will reduce the risk of interference with the cloning process.

7 If you want to use the actual HDD to perform Neoware UbiBoot hardware detection, run Neoware UbiBoot now (assuming default installation, from the **Start** menu select **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware UbiBoot**).

As Active Cloner clones the current logical partition, you do not have to use a particular write mode if you run Active Cloner just after having run UbiBoot. Neoware UbiBoot modifies the system actually running and this modified system will be cloned.

8 If the actual HDD is physically connected to another computer on your local network, you must share this hard drive's root folder and connect this shared folder to the Neoware Image Manager client that runs Active Cloner, so that this shared hard drive is assigned a drive letter on the client. You can use the `net use` command to achieve this.

Launch Neoware Active Cloner. For example, if the target partition is `E:` and `NIMCloner.exe` is located in `C:\Program Files\Neoware\Image_Manager_4.6\Client\tools`, type the following:

```
C:
cd \Program Files\Neoware\Image_Manager_4.6\Client\
tools\NIMCLONER E:
```

if the target partition is `D:` and `NIMCloner.exe` stands in `\\MYSERVER\NIMCLONER`, type the following:

```
\\MYSERVER\NIMCLONER\NIMCLONER E:
```

Neoware Active Cloner will dump the contents of the actual system partition used to boot the client onto the target partition in the actual local hard disk. It uses an incremental cloning system so that files that are the same in the source and the target partition are not actually copied. This makes upgrades to the target partition very efficient and fast.

If errors or problems are encountered while Neoware Active Cloner runs, messages are displayed. Note that errors relating to temporary or log files not being able to be copied are usually not severe and can be ignored.

Once the target partition is actually copied and is the exact image of the current system partition, the client computer can be shutdown. The actual HDD can then be used to boot the client computer (or another computer, especially if Neoware UbiBoot had been run before cloning), and a Neoware Image Manager virtual volume can be created after the primary partition in this actual HD, using the Client Builder tool.

For a detailed description of Neoware Active Cloner, refer to the chapter “Neoware Active Cloner” on page 271.

CHAPTER 14

Adding Clients to Windows Domains

This chapter describes how to add Neoware Image Manager clients to a Windows domain using the Neoware Domain Wizard.

Introduction

The Neoware Domain Wizard `NeoDomain.exe` enables you to add Image Manager clients to a Windows domain. This wizard modifies the disk image so that domain membership is available for multiple computers using the same image as their system virtual hard disk. The Windows domain controllers can be Windows NT (3.51/4.0), Windows 2000/2003 (Active Directory or NT4 style), or Samba.

How the Neoware Domain Wizard Works

The Neoware Domain Wizard is able to use personalized domain credentials for each client that boots off the same shared image. The wizard stores the domain credentials for each client in a repository. It then uses the correct credentials when a client connects to a domain. The repository where Domain Credentials are stored can be either:

- A directory on the NVDD server
- In the System Drive (the shared image itself)
- On an extra drive

Domain Credentials are stored when the client computer shuts down. When a client computer boots off a shared virtual HD it will use its own personalized Domain Credentials.

Repository for Domain Credentials

The Neoware Domain Wizard can store the domain credentials for each member either in a directory on the server (default), the system partition, or in another partition.

Repository in a Server Directory

Domain credentials can be stored at shutdown directly onto the NVDD server, in a directory named using the client's MAC address. The domain credentials will be loaded from this directory at boot time.

The root directory where the client directories are created can be defined in the `nvdd` configuration file with the line (global parameter):

```
client_files_dir=<path>
```

You can also specify the client files directory in the Neoware Image Manager Console using the **Client files folder** option (select **Generic options** in the **Tools** menu, then click the **Directories** tab).

This parameter is set to "." by default (the working directory of the NVDD server).

Note: *The NVD protocol file transfer feature can only enable the storage and loading of domain credentials from a subdirectory named after the client's MAC address, and this subdirectory must be in the directory specified by the* `client_files_dir=<path>` *line in the nvdd configuration file.*

Repository in the System Partition

When the domain credentials are stored in the system partition and this partition is mounted in CVolwrite/Volatile mode, it is recommended that you disable the password renewal policy. This is because if a new password is elected by the client and the server, it

will not be saved with the domain credentials because the system Virtual HD is mounted in CVolwrite/Volatile mode. The domain controllers will assume that the client knows its new password when this password has actually been forgotten by the client when it rebooted.

The Neoware Domain Wizard will automatically disable Machine Accounts Passwords changes when the **Repository in System Partition** option is selected.

Repository in a Non-System Partition

When the domain credentials are not stored in the system partition and the system partition is mounted in CVolwrite/Volatile mode by the clients, the partition where the domain credentials are stored can be mounted in CVolwrite/Normal mode. The domain credentials can even be stored in a hard disk partition.

If the partition used to store the domain credentials is in a Neoware Image Manager virtual volume, the recommended write mode for this volume is CVolwrite/Normal. This will allow each client to have its own domain credentials in its own CVol file.

If you want to use an additional Neoware Image Manager Virtual HD as the repository to store domain credentials, it is recommended that you use a copy of `smalldisk.vol` drive and to make it available as a non-boot drive to every client computer that will be a member of the domain. In normal operations, this small HD volume should be mounted in Normal mode (CVolwrite/Normal).

The administrator can specify any folder in this drive to be used as the repository for domain credentials.

In CVolwrite/Normal mode, the personalized data on a drive is retained after a reboot. So when the machine account password changes it will be retained by both the client (Machine Domain Account Password is part of domain credentials) and the Domain Controller.

Same Repository used by Different Shared System HD Images

When the repository is stored on a Neoware Image Manager server or in a separate drive, the domain credentials can be associated with different shared system HD images that have been created from a common "strain" image. This is because the domain credentials depend on data contained in the image itself. As long as the clients always get the same computer name, they can use the *same* domain credentials with different images. In this case, when the domain credentials are stored on the Neoware Image Manager server, it is recommended that the different hard disk images are shared using the same server configuration file. This will ensure that the client files directory and client names are consistent for each image.

If you want to use several images and you also want the clients to be members of a domain, the recommended procedure is as follows:

1. Create one image with the common set of components that will be used by all your images. This is your common or basic image.
2. Use the standard procedure to add the clients to the domain with this common image.
3. Duplicate this image as many times a needed in order to create the desired number of images.
4. Modify separately each image (in Admin mode or by merging CVol files into the image).

Note that you can use several images with the same set of clients even if the images are not coming from a common strain image, as long as only one image is configured so that Image Manager will process the domain credentials. If you do not activate any repository for domain credentials in a specific image (and thus the clients using this image in volatile mode cannot be members of a domain), there will be no problem making this image co-exist with a domain-enabled image.

For example, if the user can choose from three different Windows XP Pro images at boot time (e.g. Windows XP-Pro Back-Office, Windows XP-Pro Diagnotic, Windows XP-Pro Open access), the

client computer can still be a member of the domain and use the same domain credentials no matter which HD image was used to boot up the computer.

Another application of this unique feature is when the Administrator changes the unique HD image that is assigned to a client computer as its system image. For example, the system image is changed from `WindowsXP-Pro-Diag.vol` to `WindowsXP-Pro-Office.vol`. Both images are made for clients that are members of the same domain and come from a common strain image. When the system HD image changes, the domain credentials in the repository do not change. The same domain credentials will be used whatever the system image. As the client computers get the same name (from the Neoware Image Manager server or DHCP), the same domain credentials must be used (Domain Controllers and Domain Members use client name as the identifier for joining a domain); this is made possible because the domain credentials are the same whatever the system HD image. This is not possible with standard HD based Windows systems.

Storing Domain Credentials in an NVDD Server Directory

Windows XP Professional Clients

The following procedure requires that you use the Windows XP Professional client operating system.

Before you perform the following procedure, make sure that the client computer *is not* a member of a domain. If it is a member of a domain, you must remove it before you continue.

Once the client computers boot correctly with Neoware Image Manager, do the following:

1 Backup the hard disk image on the server.

You can copy the image to another image file that you will modify. You can copy an image currently used by clients as long as it is not currently used in Admin mode.

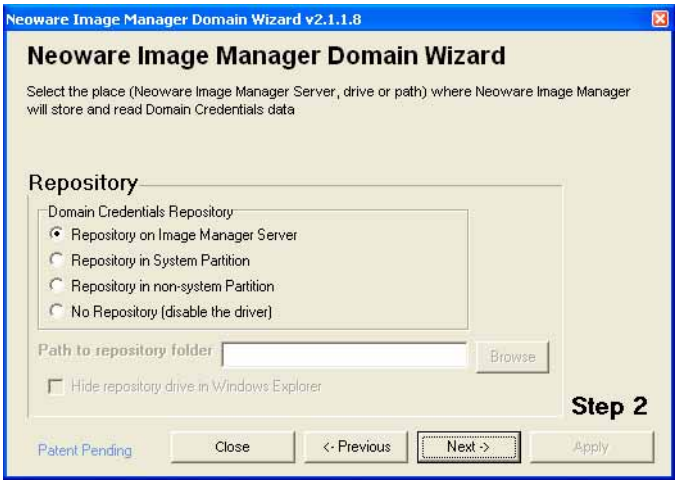
2. Shutdown all the clients that are using the image you will be modifying. If you will be working on a copy of an image created in the previous step, make sure that no clients are using that image.
3. Use the Neoware Image Manager Console to change the default writing mode for the virtual system volume (the volume usually mounted as `C:` on your clients) to Admin mode.
4. Save the `nvdd` configuration file in the Image Manager Console.
5. Reload the `nvdd` configuration file in the Image Manager Console so that the writing mode changes are taken into account.
6. Boot *ONE* client allowed to open the image in Admin mode.
7. Log on this client using an *Administrator Local User Account* (a user account local to this client user's database with administrative rights). You cannot use a domain user account because your client is not a member of a domain.
8. On this client, launch the Neoware Domain Wizard either from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Domain Wizard**, or by running the executable file `NeoDomain.exe` (usually stored in the subdirectory `Client\NeoDomMgr` of the Neoware software distribution package).

   The file `NeoDomMgr.sys` must be stored in the same directory from which `NeoDomain.exe` is run.

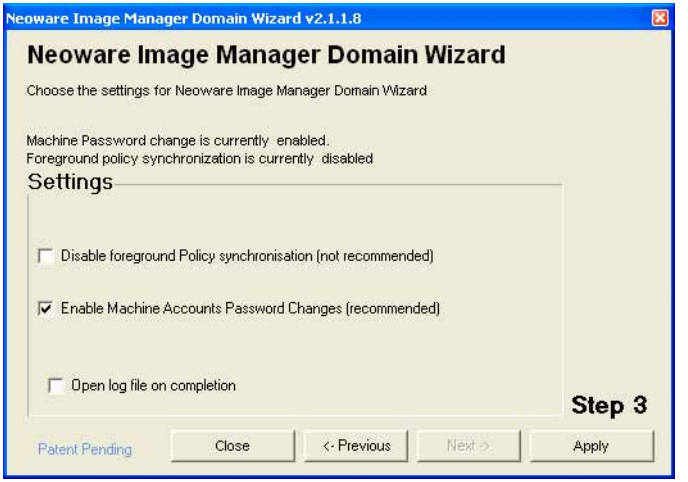
   The following window will be displayed.

Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
This tool is intended to install some components related to Windows Domain membership management, in Neoware Image Manager™
You must run this tool on ONE diskless remote booted client, with Neoware Image Manager system volume mounted in Admin mode. If you want to store Domain Credential on non volatile olume, a secondary volume must be mounted in non-volatile mode.
Step 1
Patent Pending
Close
<- Previous
Next ->
Apply

9 Click **Next** to continue.


Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
Select the place (Neoware Image Manager Server, drive or path) where Neoware Image Manager will store and read Domain Credentials data
Repository
Domain Credentials Repository
Repository on Image Manager Server
Repository in System Partition
Repository in non-system Partition
No Repository (disable the driver)
Path to repository folder
Browse
Hide repository drive in Windows Explorer
Step 2
Patent Pending
Close
<- Previous
Next ->
Apply

10 Select the option **Repository on Image Manager server** (default) then click **Next**.


Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
Choose the settings for Neoware Image Manager Domain Wizard
Machine Password change is currently enabled.
Foreground policy synchronization is currently disabled
Settings
Disable foreground Policy synchronisation (not recommended)
Enable Machine Accounts Password Changes (recommended)
Open log file on completion
Step 3
Patent Pending
Close
<- Previous
Next ->
Apply

11 If you use CVolwrite/Volatile mode for your system Virtual HD, you should keep the default options.

12 Click **Apply** to continue.

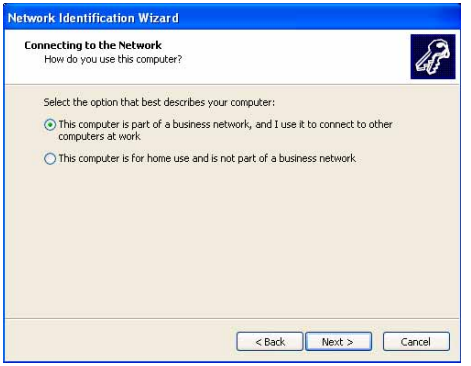
You will see the message **Operation completed** in the Neoware Domain Wizard window.

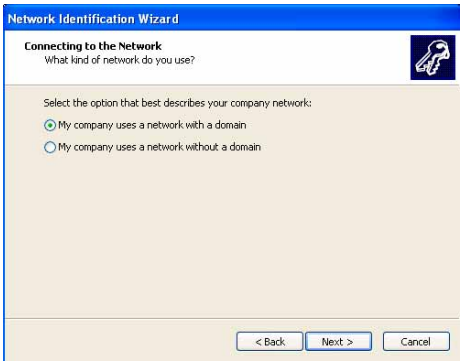
13 Make sure that the client preferred DNS IP address is set to a Domain Controller IP address. You may need to tune your DHCP options in order to set the correct preferred DNS Server. If you are told that there are several network cards with the same IP address in the client computer, click the **No** button and leave the system as it is.

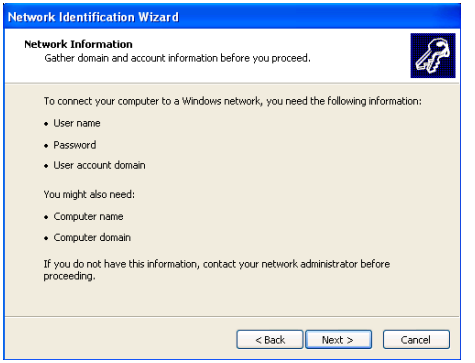
14 On the client, open **System Properties** (**Control Panel** > **System**). Click the **Computer Name** tab, then click the **Network ID** button.

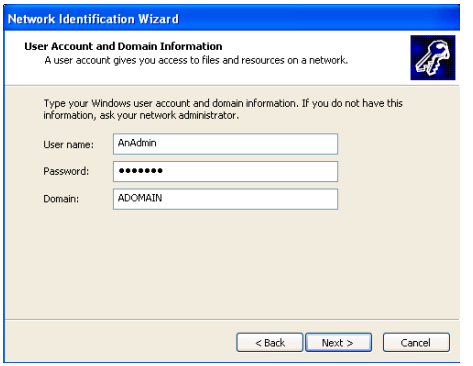
15 Configure your client so that it becomes a member of your domain. The following screen captures illustrate the usual method for joining clients in a domain using the Network Identification Wizard.

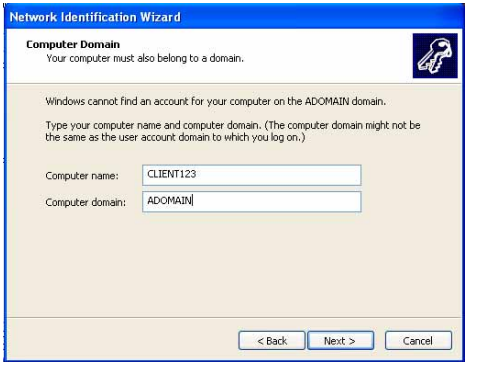
Network Identification Wizard
Welcome to the Network Identification Wizard
This wizard helps you connect your computer to a network.
To continue, click Next.
< Back
Next >
Cancel


Network Identification Wizard
Connecting to the Network
How do you use this computer?
Select the option that best describes your computer:
This computer is part of a business network, and I use it to connect to other computers at work
This computer is for home use and is not part of a business network
< Back
Next >
Cancel

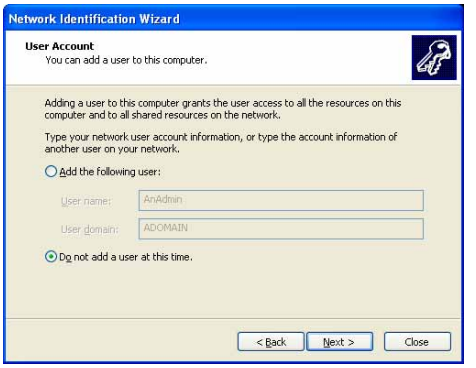

Network Identification Wizard
Connecting to the Network
What kind of network do you use?
Select the option that best describes your company network:
My company uses a network with a domain
My company uses a network without a domain
< Back
Next >
Cancel

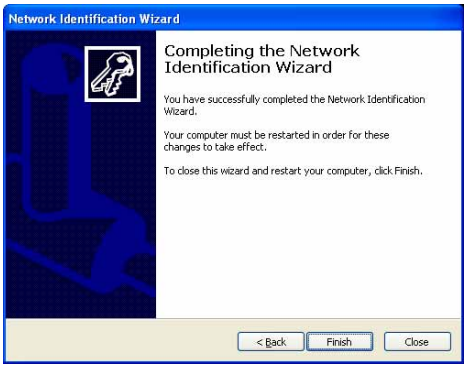

Network Identification Wizard
Network Information
Gather domain and account information before you proceed.
To connect your computer to a Windows network, you need the following information:
• User name
• Password
• User account domain
You might also need:
• Computer name
• Computer domain
If you do not have this information, contact your network administrator before proceeding.
< Back
Next >
Cancel


Network Identification Wizard
User Account and Domain Information
A user account gives you access to files and resources on a network.
Type your Windows user account and domain information. If you do not have this information, ask your network administrator.
User name:
AnAdmin
Password:
•••••••
Domain:
ADOMAIN
< Back
Next >
Cancel


Network Identification Wizard
Computer Domain
Your computer must also belong to a domain.
Windows cannot find an account for your computer on the ADOMAIN domain.
Type your computer name and computer domain. (The computer domain might not be the same as the user account domain to which you log on.)
Computer name:
CLIENT123
Computer domain:
ADOMAIN
< Back
Next >
Cancel

Domain User Name and Password
Type the name and password of an account with permission to join the domain.
User name:
AnAdmin
Password:
Domain:
ADOMAIN
OK
Cancel


Network Identification Wizard
User Account
You can add a user to this computer.
Adding a user to this computer grants the user access to all the resources on this computer and to all shared resources on the network.
Type your network user account information, or type the account information of another user on your network.
Add the following user:
User name:
AnAdmin
User domain:
ADOMAIN
Do not add a user at this time.
< Back
Next >
Close


Network Identification Wizard
Completing the Network Identification Wizard
You have successfully completed the Network Identification Wizard.
Your computer must be restarted in order for these changes to take effect.
To close this wizard and restart your computer, click Finish.
< Back
Finish
Close

Computer Name Changes
You must restart this computer for the changes to take effect.
OK

16. When needed, provide the domain administrative account user name and password. If a computer account already exists in the domain for the client, you can re-use this account.
17. Reboot the computer.
18. Log on to the client computer *using any Domain Account.*
19. Shutdown the client computer.
20. Use the Image Manager Console to change the default writing mode for the virtual volume to CVolwrite/Volatile mode. Reload the `nvdd` configuration file in the Image Manager Console so that the writing mode changes are taken into account.
21. Boot one other client.
22. Log on this client using an *Administrator Local User Account* (a user account local to this client users database with administrative rights), not a domain user account.
23. On the client, open **System Properties** (**Control Panel** > **System**). Click on the **Network ID** button. Join the computer to the domain as you did previously.
24. Reboot the client computer and log in with a Domain User account.
25. Shutdown the client computer.
26. Repeat steps 20-26 until all the required client computers' accounts are created.
27. Shutdown the last client.
28. Start all the clients.
29. At the Windows login prompt choose to log on the domain.

You can now enjoy domain related features (roaming profiles, centralized user account management... etc.)

Windows 2000 Professional Clients

The procedure is the same as for Windows XP Professional clients described in the previous section, except that there is no Network ID wizard in Windows 2000. Instead, you have to do the following to replace Network ID wizard operations:

1. Run the **Control Panel** > **System** applet.
2. Select the **Computer Name** tab.
3. Click the **Change** button.
4. If the client is indicated to be a member of a domain, make it a member of a workgroup. Do not reboot when Windows asks you to reboot.
5. Select the **Domain** option to add the client into the domain. Provide user credentials as needed (you must provide the credentials of a user that can add and remove computers in the desired domain).
6. Validate each step until Windows asks you to reboot.
7. Reboot the client computer.

Client Names

As domain controllers use the client name to retrieve the security data relative to each client so that it can connect to the domain, it is required that each client always get the same name. To achieve this you can use client host name and static DHCP entries (DHCP reservations). If a client name changes, it must be added to the domain again.

Adding a New Client to the Domain

When you need to add a new client computer to the domain, if the Neoware Domain Wizard has already been applied to the virtual volume, you do not need to re-apply it. You just need to make the new client computer boot on the virtual volume in the same way that you added the clients previously. Use the Network Identification Wizard, just as you did for the other clients.

It is possible to add Neoware Image Manager clients to the domain without having to sit in front of each client to perform domain membership subscription.

It is possible to use automated scripts that use the Microsoft `netdom` utility in order to perform the "join domain" task.

`Netdom` for Windows 2000 sp4 clients is available at the following Internet address:

`http://www.microsoft.com/windows2000/downloads/service-packs/SP4/supporttools.asp`

`Netdom` for Windows XP sp2 clients is available at the following Internet address:

`http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en`

The following is an example of a startup script for automatically joining clients to a domain:

```
net start workstation
set verif=0

SET DomainName=ADomain
SET UserName=AnAdmin
SET UserPass=s3cr3tp4ssw0rd

netdom.exe verify %computername% /Domain:%DomainName%

IF %ERRORLEVEL% NEQ 0 (
   set verif=1
   netdom.exe join %computername% /Domain:%DomainName%
              /Userd:%UserName% /Passwrdd:%UserPass%
)

IF %verif% EQU 1 (
   IF %ERRORLEVEL% EQU 0 (
       Shutdown -f -r -t 120
     goto end
   )
)

:end
SET DomainName=
SET UserName=
SET UserPass=
```

In order for such a script to work, you have to make sure that:

- `netdom.exe` is in the system search path (for example, copy it in `c:\windows\system32`).
- the Environment variables `DomainName`, `UserName` and `UserPass` are consistent. (`UserName` must be the name of a user account in the domain specified by `DomainName`. `UserName` must have the right to add and remove computers in `DomainName`.)
- the settings of the Windows instance contained in your image are such that the service NetLogon is started automatically.
- this script is launched before the login dialog is displayed. To achieve this, use a computer startup script that you would set using the Group Policy editor (`gpedit.msc`) run on a client that had mounted the image in Admin mode.
- there is no pre-existing `NeoDomSO` file (where the domain credentials are stored) for the client that has to be added to the domain. These files are usually stored in a folder named with the client's MAC address in the folder specified by the `client_files_dir` parameter.

Note that this script can stay in the image even after the clients are joined to the domain. Then, when you add a new client, all you have to do is make sure that it gets the name you specified (e.g. in the Image Manager console). It will boot once and join the domain, then reboot and be a member of the domain.

Storing Domain Credentials on a Non-Volatile Drive

The following procedure requires that you use the Windows 2000 Professional or Windows XP Professional operating system.

Before you perform the following procedure, make sure that the client computer *is not* a member of a domain. If it is a member of a domain, you must remove it before you continue.

Once the client computers boot correctly with Neoware Image Manager, do the following:

1. Backup the hard disk image on the server.

   You can copy the image to another image file that you will modify. You can copy an image currently used by clients as long as it is not currently used in Admin mode.

2. Shutdown all the clients that are using the image you will be modifying. If you will be working on a copy of an image created in the previous step, make sure that no clients are using that image.

3. Use Neoware Image Manager Console to change the default writing mode for the virtual system volume (the volume usually mounted as `C:` on your clients) to Admin mode.

4. If you want to store the domain credentials in a Neoware Image Manager virtual HD, modify the Neoware Image Manager server configuration so that the clients will mount an extra drive. Set the relevant writing mode so that your clients will mount this extra virtual HD in Admin mode. This virtual HD should not be set as a bootable HD. You can use a copy of `smalldisk.vol` as this secondary volume. The size of `smalldisk.vol` is 8MB which is enough for domain credentials. If the repository is on hard disks local to each client computer, you must make sure that all these hard disks will be mounted with the same driver letter on every client. Note that using USB-Keys or USB disks to store the domain credentials is not possible.

5. Save the `nvdd` configuration file in Neoware Image Manager Console.
6. Reload the `nvdd` configuration file in Neoware Image Manager Console so that the writing mode changes are taken into account.
7. Boot *ONE* client.
8. Log on this client using an *Administrator Local User Account* (a user account local to this client user's database with administrative rights). You cannot use a domain user account because the client is not a member of a domain.
9. Check that you can actually access the new extra drive. (Use Windows Explorer, check that the extra drive is present and that you can create and delete files or directories on it.)
10. *Reboot the client computer.* (This step is important, do not miss it!)
11. Log on this client using an *Administrator Local User Account* (a user account local to this client user's database with administrative rights).
12. On this client, launch the Neoware Domain Wizard either from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Domain Wizard**, or by running the executable file `NeoDomain.exe` (usually stored in the subdirectory `Client\NeoDomMgr` of the Neoware software distribution package).

    The files `NeoDomMgr.sys` and `License.txt` must be stored in the same directory from which `NeoDomain.exe` is run.

    The following window will be displayed.

Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
This tool is intended to install some components related to Windows Domain membership management, in Neoware Image Manager™
You must run this tool on ONE diskless remote booted client, with Neoware Image Manager system volume mounted in Admin mode. If you want to store Domain Credential on non volatile olume, a secondary volume must be mounted in non-volatile mode.
Step 1
Patent Pending
Close
<- Previous
Next ->
Apply

13 Click **Next** to continue.

Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
Select the place (Neoware Image Manager Server, drive or path) where Neoware Image Manager will store and read Domain Credentials data
Repository
Domain Credentials Repository
Repository on Image Manager Server
Repository in System Partition
Repository in non-system Partition
No Repository (disable the driver)
Path to repository folder
D:\Domain
Browse
Hide repository drive in Windows Explorer
Step 2
Patent Pending
Close
<- Previous
Next ->
Apply

14 Select the option **Repository in non-system Partition**.

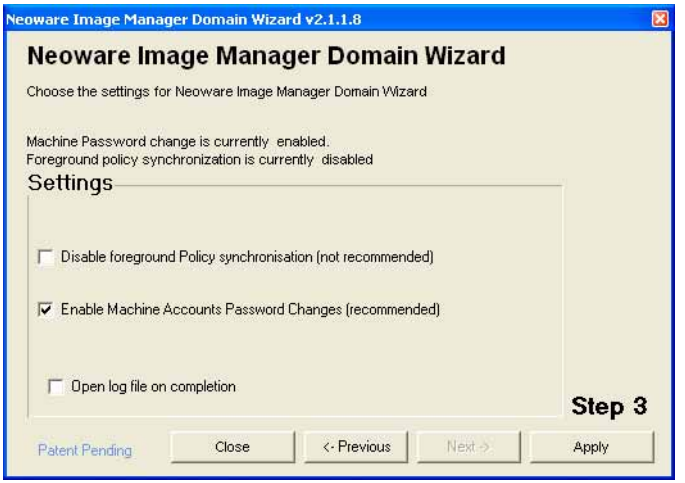
15 In the field **Path to repository folder**, enter the path of the directory in which you do want the domain credentials to be stored

(e.g. `D:\`). Note that you can only choose a directory on an existing drive as the path to repository folder.

If you check the option **Hide repository drive in Windows Explorer**, the drive on which the repository is housed will not appear in Windows explorer. This uses the `NoDrive` registry feature of Windows. For more details about `NoDrive`, refer to:

`http://www.windowsitpro.com/Article/ArticleID/37880/37880.html?Ad=1`

16 Click **Next** to continue.


Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
Choose the settings for Neoware Image Manager Domain Wizard
Machine Password change is currently enabled.
Foreground policy synchronization is currently disabled
Settings
Disable foreground Policy synchronisation (not recommended)
Enable Machine Accounts Password Changes (recommended)
Open log file on completion
Step 3
Patent Pending
Close
<- Previous
Next ->
Apply

17 If you plan to use CVolwrite/Volatile mode for your system Virtual HD when it is used in production, you should keep the default options.

Refer to the following web sites for information on the Foreground Policy option:

`http://support.microsoft.com/kb/q305293/`

`http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/274e614e-f515-4b80-b794-fe09b5c21bad.mspx`

18 Click **Apply** to continue.

You will see the message **Operation completed** in the Neoware Domain Wizard window.

19 Make sure that the client preferred DNS IP address is set to a Domain Controller IP address. You may need to tune your DHCP server options in order to set the preferred DNS server for your clients. If you are told that there are several network cards with the same IP address in the client computer, click the **No** button and leave the system as it is.

20 On the client, open **System Properties** (**Control Panel** > **System**). Click on the **Computer Name** tab then click the **Change** button.

21 Check the **Domain** option so that the computer is made a member of a domain. Provide the domain name. If needed, provide the domain administrative account user name and password. If a computer account already exists in the domain for the client, you can re-use this account.

22 Change the write mode for the extra volume (the one that stored Domain Credentials) to CVolwrite/Normal and reload the configuration on the server side. Reload the configuration file so that Neoware Image Manager server takes this new setting into account.

23 Reboot the computer.

24 Log on to the client computer *using any Domain Account.*

25 Shutdown the client computer.

26 Use the Neoware Image Manager Console to change the default writing mode for the virtual system volume (the volume usually mounted as `C:` on your clients) to CVolwrite/Normal mode, or CVolwrite/Volatile mode if you know that you can remove client computers from the domain and insert them again without rebooting (refer to the following sections).

27 Save the `nvdd` configuration file in the Image Manager Console.

28 Reload the nvdd configuration file in the Image Manager Console so that the writing mode changes are taken into account.

29 Boot one other client.

30 Log on this client using an *Administrator Local User Account* (a user account local to this client user's database with administrative rights). Do not use a domain user account.

31 On the client, open **System Properties** (**Control Panel** > **System**). Click on the **Computer Name** tab then click the **Change** button.

32 Change the Domain options so that the computer is made a member of a WORKGROUP and not a domain anymore. Provide the workgroup name (use the Domain name as the workgroup name). If needed, provide the domain administrative account user name and password. Click the **OK** buttons until the system properties windows close.

33 *Optional, if you validated it (refer to the section "Do I Need to Reboot?" on page 169):* Reboot the computer as Windows asks.

34 If you rebooted in the previous step, log on this client using an *Administrator Local User account*. Open **System Properties** (**Control Panel** > **System**). Click on the **Computer Name** tab then click the **Change** button.

35 Check the **Domain** option so that the computer is made a member of a domain. Provide the domain name. If needed, provide the domain administrative account user name and password. If a computer account already exists in the domain for the client, you can re-use this account.

36 Reboot the client computer and log in with a Domain User account.

37 Shutdown the client computer.

38 Repeat steps 29-38 until there are no more clients to add to the domain.

39 *Optional, depending on the "no-need for reboot" validation (refer to the section "Do I Need to Reboot?" on page 169):* Use the Neoware Image Manager Console to change the default writing mode for the virtual system volume (the volume usually mounted as `C:` on your clients) to CVolwrite/Volatile. Save the `nvdd` configuration file in the Image Manager Console. Reload the `nvdd` configuration file in the Image Manager Console so that the writing mode changes are taken into account.

40 Now, at the Windows login prompt, you can choose to log on the domain.

You can now enjoy domain related features (roaming profiles, centralized user account management... etc.).

Client IP Addresses

If the domain credentials are stored in a Neoware Image Manager virtual HD, the Neoware Domain Wizard uses the client IP address to retrieve the security data relative to each client. This data makes it possible for the client to connect to the domain (the personalized data are stored in a CVol file that uses the client IP address). It is therefore essential that each client always get the same IP address. To achieve this you can use client host name and static DHCP entries (DHCP reservations). If a client IP address changes, it must be added to the domain again.

Adding a New Client to the Domain

When you need to add a new client computer to the domain, if the Neoware Domain Wizard has already been applied to the virtual volume, you do not need to re-apply it. You just need to make the new client computer boot on the virtual volume in the same way that you added the clients previously. Make sure that this client has access to the disk where the Domain Credentials are stored, then make this client leave the domain and join it again, just as you did for the other clients.

It is possible to add Neoware Image Manager clients to the domain without having to sit in front of each client to perform domain membership subscription. You can use the Microsoft resource tool `netdom` and perform the steps **Remove from domain / add to workgroup,**

add to domain again using scripts run by the clients when they boot-up.

It is possible to use automated scripts that use the Microsoft `netdom` utility in order to perform the "leave domain" and "join domain" tasks. `Netdom` can even be configured to reboot the computer after it has performed "leave domain" or "join domain" tasks, if you validated that this step is needed.

`Netdom` for Windows 2000 sp4 clients is available at the following Internet address:

```
http://www.microsoft.com/windows2000/downloads/service-packs/SP4/supporttools.asp
```

`Netdom` for Windows XP sp2 clients is available at the following Internet address:

```
http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en
```

Do I Need to Reboot?

Usually, depending on each system configuration, you do not need to reboot after the client leaves the domain and before it can join it again. However, it has been reported that joining a domain has failed when you have not rebooted, while it succeeded when it has been rebooted and the client opened the System volume in CVolwrite/Normal mode during the leave/join domain operation.

All that we can recommend is that you do your own tests. Testing domain integration without rebooting can be done as follows:

- After you added the first client to the domain, change the default writing mode to CVolwrite/Volatile.
- Use at least 3 client computers. If you use less than 3 clients, the test is not relevant.
- Try to remove the clients from the domain and then join them to the domain again without rebooting between the leave domain and join domain step.

- Try to log on to each of these client computers with Domain User credentials.

If you can log on these clients using Domain User name and password, you do not need to reboot between removing and joining each client to the domain again.

Storing Domain Credentials in the System Partition

The following procedure requires that you use the Windows 2000 Professional or Windows XP Professional operating system.

When you run Client Builder to build the image of the Reference HD, the client computer must not be a member of a domain.

Once the client computers boot correctly with Neoware Image Manager, do the following:

1. Backup the hard disk image on the server.

   You can copy the image to another image file that you will modify. You can copy an image currently used by clients as long as it is not currently used in Admin mode.

2. Shutdown all the clients that are using the image you will be modifying. If you will be working on a copy of an image created in the previous step, make sure that no clients are using that image.

3. Use the Neoware Image Manager Console to change the default writing mode for the virtual system volume (the volume usually mounted as `C:` on your clients) to Admin mode.

4. Save the `nvdd` configuration file in the Image Manager Console.

5. Reload the `nvdd` configuration file in the Image Manager Console so that the writing mode changes are taken into account.

6. Boot *ONE* client.

7 Log on this client using an *Administrator Local User Account* (a user account local to this client user's database with administrative rights). Do not use a domain user account.

8 On this client, launch the Neoware Domain Wizard either from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Domain Wizard**, or by running the executable file `NeoDomain.exe` (usually stored in the subdirectory `Client\NeoDomMgr` of the Neoware software distribution package).

The files `NeoDomMgr.sys` and `License.txt` must be stored in the same directory from which `NeoDomain.exe` is run.

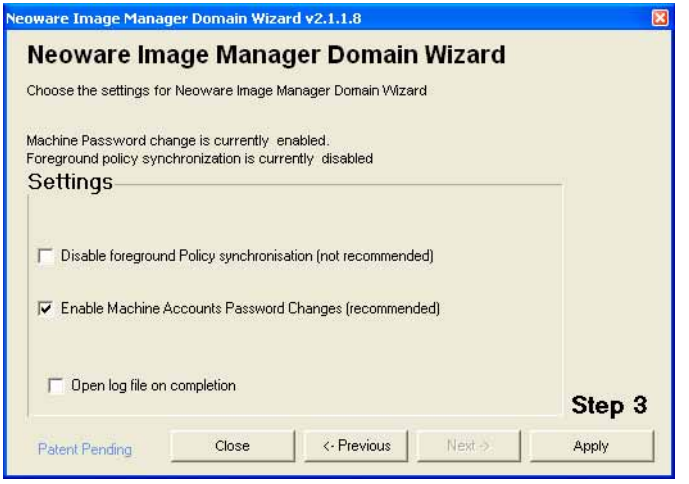
The following window will be displayed.

Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
This tool is intended to install some components related to Windows Domain membership management, in Neoware Image Manager™
You must run this tool on ONE diskless remote booted client, with Neoware Image Manager system volume mounted in Admin mode. If you want to store Domain Credential on non volatile olume, a secondary volume must be mounted in non-volatile mode.
Step 1
Patent Pending
Close
<- Previous
Next ->
Apply

9 Click **Next** to continue.

Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
Select the place (Neoware Image Manager Server, drive or path) where Neoware Image Manager will store and read Domain Credentials data
Repository
Domain Credentials Repository
Repository on Image Manager Server
Repository in System Partition
Repository in non-system Partition
No Repository (disable the driver)
Path to repository folder
Browse
Hide repository drive in Windows Explorer
Step 2
Patent Pending
Close
<- Previous
Next ->
Apply

10 Select the option **Repository in System Partition** then click **Next**.


Neoware Image Manager Domain Wizard v2.1.1.8
Neoware Image Manager Domain Wizard
Choose the settings for Neoware Image Manager Domain Wizard
Machine Password change is currently enabled.
Foreground policy synchronization is currently disabled
Settings
Disable foreground Policy synchronisation (not recommended)
Enable Machine Accounts Password Changes (recommended)
Open log file on completion
Step 3
Patent Pending
Close
<- Previous
Next ->
Apply

11 If you use CVolwrite/Volatile mode for your system Virtual HD, you should keep the default options.

Refer to the following web sites for information on the Foreground Policy option:

`http://support.microsoft.com/kb/q305293/`

`http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/274e614e-f515-4b80-b794-fe09b5c21bad.mspx`

12 Click **Apply** to continue.

You will see the message **Operation completed** in the Neoware Domain Wizard window.

13 Make sure that the client preferred DNS IP address is set to a Domain Controller IP address. You may need to tune your DHCP options in order to set the correct preferred DHCP Server. If you are told that there are several network cards with the same IP address in the client computer, click the **No** button and leave the system as it is.

14 On the client, open **System Properties** (**Control Panel** > **System**) and click the **Change** button.

15 Check the **Domain** option so that the computer is made a member of a domain. Provide the domain name. If needed, provide the domain administrative account user name and password. If a computer account already exists in the domain for the client, you can re-use this account.

16 Reboot the computer.

17 Log on to the client computer *using any Domain Account.*

18 Shutdown the client computer.

19 Boot one other client, or the same client after having changed its computer name. In the second case, you will need to change the computer name in the Neoware Image Manager configuration, or in DHCP settings, so that the computer name gets the new name when it boots. (Refer to the section “Client Names” on page 174 for details.)

20 Log on this client using an *Administrator Local User Account* (a user account local to this client users database with administrative rights), not a domain user account.

21 Repeat steps 13-20 until all the required client computers' accounts are created.

22 Shutdown the last client.

23 Use the Image Manager Console to change the default writing mode for the virtual volume to CVolwrite/Volatile mode (or CVolwrite/Normal mode if this suits your requirements).

24 Save the `nvdd` configuration file in the Image Manager Console.

25 Reload the `nvdd` configuration file in the Image Manager Console so that the writing mode changes are taken into account.

26 Start all the clients.

27 At the Windows login prompt choose to log on the domain.

You can now enjoy domain related features (roaming profiles, centralized user account management... etc.).

Client Names

As domain controllers use the client name to retrieve the security data relative to each client so that it can connect to the domain, it is required that each client always get the same name. To achieve this you can use Neoware Image Manager client naming or DHCP client host name and static DHCP entries (DHCP reservations). If a client name changes, it must be added to the domain again.

Adding a New Client to the Domain

When you need to add a new client computer to the domain, if the Neoware Domain Wizard has already been applied to the virtual volume, you do not need to re-apply it. You just need to make the new client computer boot on the virtual volume in Admin mode to make it a member of the domain (log on with Local Administrator account, make it leave the domain, reboot it, join it to the domain) and then reboot it once.

It is possible to add Neoware Image Manager clients to the domain without having to sit in front of each client to perform domain membership subscription. You can just use one client PC to add all the clients into the domain. All that is required is that the clients' computer names are added to the domain. Then, using the same client PC, change its name in Neoware Image Manager server or DHCP configuration between each reboot and add the new client name to the domain as described earlier.

You can use the `netdom` tool from the Windows Resource Kit to create automated scripts that can be used to add/remove clients to/from a domain. Refer to the relevant Resource Kit documentation for more details about the `netdom` tool.

CHAPTER 15

Merging Image & CVol Files

This chapter describes how to use the CVolMerge tool to create a new hard disk image from an existing image and a CVol file.

Introduction

The `CVolMerge` tool enables you to create a new hard disk image file from an existing image and a CVol file, or update an existing image with the content of a CVol file. In the new hard disk image file, the sectors in the existing image file are replaced by the corresponding sectors in the CVol file. The size of the CVol file can be reduced by using the `CVolCompactor` tool before merging the two files.

Assuming default **Server** installation, the `CVolMerge` and `CVolCompactor` executable files can be found in the following directory:

```
C:\Program Files\Neoware\Image_Manager_4.6\
Server\Tools
```

Assuming default **Decompress** installation, the `CVolMerge` and `CVolCompactor` executable files can be found in one of the following directories:

```
C:\Program Files\Neoware\Image_Manager_4.6\Server\
Windows\Tools
```

```
C:\Program Files\Neoware\Image_Manager_4.6\Server\
Linux\Dynamic\Tools
```

```
C:\Program Files\Neoware\Image_Manager_4.6\Server\
Linux\Static\Tools
```

```
C:\Program Files\Neoware\Image_Manager_4.6\Server\
FreeBSD\Dynamic\Tools
C:\Program Files\Neoware\Image_Manager_4.6\Server\
FreeBSD\Static\Tools
```

Using the CVolCompactor Tool

The `CVolCompactor` tool is used to reduce the size of a CVol file before merging it with a hard disk image file.

`CVolCompactor` will look at the sectors in the CVol file and compare them with the sectors in the image file. If the sectors are the same, they are removed from the CVol file. The new CVol file that is generated will only contain the sectors that are actually different from those in the image file. Note that sectors are written consecutively in the new CVol file, so it effectively defragments it. The `CVolCompactor` tool is also useful because several processes in Windows OS are actually writing the same data in the same sectors at regular intervals (registry hives, for example, are regularly dumped on the hard disk).

The syntax for the `CVolCompactor` command is as follows:

```
CVolCompactor <CVol header filename> <image filename>
<new CVol filename>
```

Windows example:

```
CVolCompactor testdisk@00E0C554E700 testdisk.vol
testdisknew@00E0C554E700
```

Using the CVolMerge Tool

The `CVolMerge` tool is used to merge the contents of a CVol file with a hard disk image file to create a new image file.

The syntax for the `CVolMerge` command is as follows:

CVolMerge <*existing HD image file path*> <*CVol file path*> *[new HD image file path]*

Please note that `CVolMerge` does not check if the parameter *`<CVol file path>`* actually refers to a CVol file relative to the hard disk image in *`<Existing HD image file path>`*.

Also, remember that the `[new HD image file]` parameter is optional; if you do not specify it, `CVolMerge` will just update the existing image file with the content of the CVol file.

Windows example:

```
CVolMerge \HDimages\big2k.vol \cvols\big2k@00E0C554E700
\HDImages\NewBig2K.vol
```

Linux/Unix example:

```
./CVolMerge /HDimages/big2k.vol/cvols/
big2k@00E0C554E700 /HDImages/NewBig2K.vol
```

CHAPTER 16

The Image Manager Console

This chapter describes how to use the Image Manager Console to change settings in an nvdd configuration file.

Introduction

The Image Manager Console provides a graphical interface for editing an `nvdd.<image filename>.conf` configuration file. Each Neoware Image Manager Server module will use its own `nvdd` configuration file that defines virtual hard disk volumes and specifies which clients can access them. Refer to the chapter "The NVDD Configuration File" on page 213 for more detailed information on the settings that the Image Manager Console enables you to modify.

Running the Image Manager Console

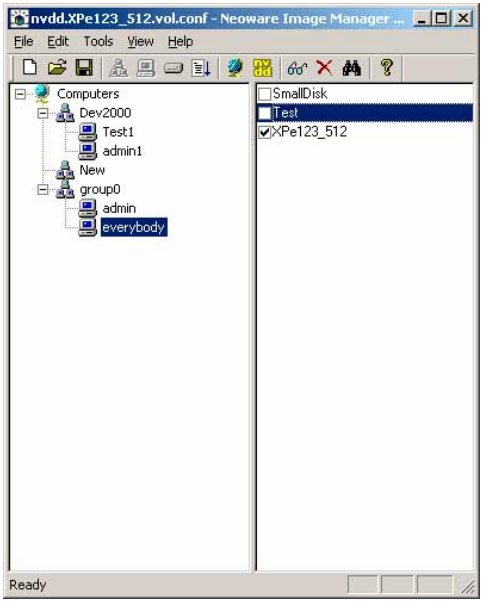
To run the Image Manager Console from the **Start** menu, select **Programs** > **Neoware** > **Image Manager** > **Neoware Image Manager Console**.

Note: *You may need to enter a password if you want to access configuration files on a remote Neoware Image Manager server. Refer to the section "Password for Remote Administration" on page 210 for details on how to set a password.*

To open a configuration file in the Console, display the **File** menu and select **Open**. Image configuration files have the file extension

`.conf`. (See later in this chapter for how to open a server configuration file of a server that is actually running, and how to reload a modified configuration file into a server that is running.)

When an image configuration file is opened in the Image Manager Console, the two panels will list the associated Clients and Volumes.



The Clients panel on the left displays the names of computers (i.e. subnets) and groups of computers. The Volumes panel on the right displays the names of all the volumes (i.e. disk images) that can be assigned to the groups of computers.

Each volume name has a check box next to it. This indicates whether the volume is assigned to the currently selected computer group. Selecting a computer or group name will indicate the volumes associated with it. You can easily select or deselect volumes for a specific group by selecting the name of the group (or a computer within it) then clicking the relevant volume check boxes.

If you want to make a computer a member of a group, just drag and drop the computer icon on the target group.

The Toolbar

The toolbar provides a quick way of accessing menu options just by clicking a button.

New
To create a new configuration file.

Open
To open an existing configuration file.

Save
To save the currently opened configuration file.

New Group
To define a new group of computers.

New Client
To define a new computer or subnet of computers.

New Volume
To define a new volume.

Merge
To merge volume details contained in another configuration file with the currently opened one.

Generic Properties
To define various properties such as network access, client overlay file directories, etc.

Nvdd Manager
To control any running Neoware Image Manager, especially remote (access, load and reload configuration files).

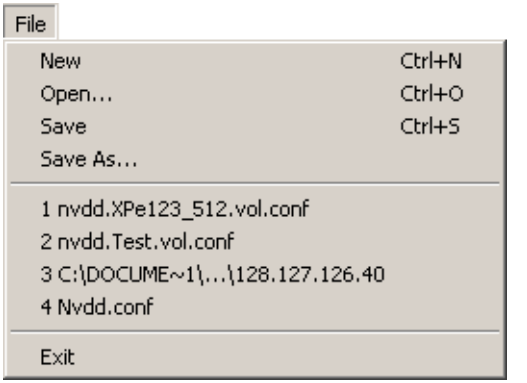
Properties
To view the properties of the selected object.

Delete
To delete the selected object.

Search
To search an object.

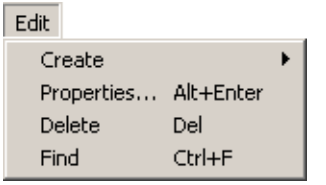
About
To open the **About** dialog.

The File Menu



The **File** menu provides standard functions for opening and saving files, and exiting the Image Manager Console.

The Edit Menu



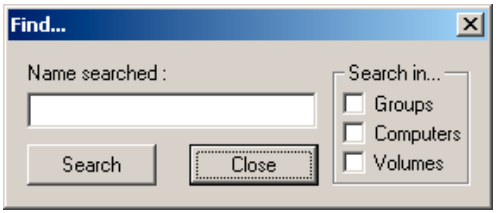
The **Edit** menu enables you to create clients and volumes, and view and edit their properties.

Selecting **Create** will display a menu enabling you to create a new **Computer**, **Group** or **Volume**. Note that you must select a corresponding object in the relevant Console panel in order to create a new version of that object. The dialogs displayed when you select these options are the same as those when you select **Properties**.

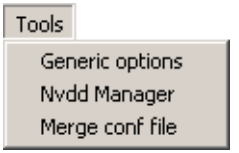
Selecting **Properties** will display a Properties dialog for the currently selected Computer, Group, or Volume. Refer to the section"Displaying & Changing Properties" on page 186 for details.

Selecting **Delete** will delete the currently selected Computer, Group, or Volume in the Console panel.

Selecting **Find** will display a dialog enabling you to search for a specified name within Groups, Computers and Volumes. This makes it easy to find an element in a large configuration file..



The Tools Menu



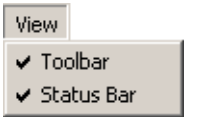
The **Tools** menu provides a set of tools for managing the Image Manager server, clients and volumes.

Selecting **Generic options** will display a dialog enabling you to specify general settings such as the default maximum CVol size, network buffer size, etc.

Selecting **Nvdd Manager** will display a dialog enabling you to connect to a running Image Manager server and open and edit configuration files on it.

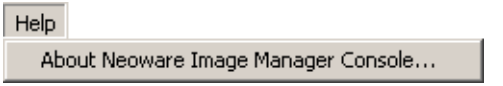
Selecting **Merge conf file** will display a dialog that enables you to open another configuration file in order to copy volume settings from it into the currently open configuration file.

The View Menu



The **View** menu enables you enable or disable display of the Toolbar and Status bar.

The Help Menu



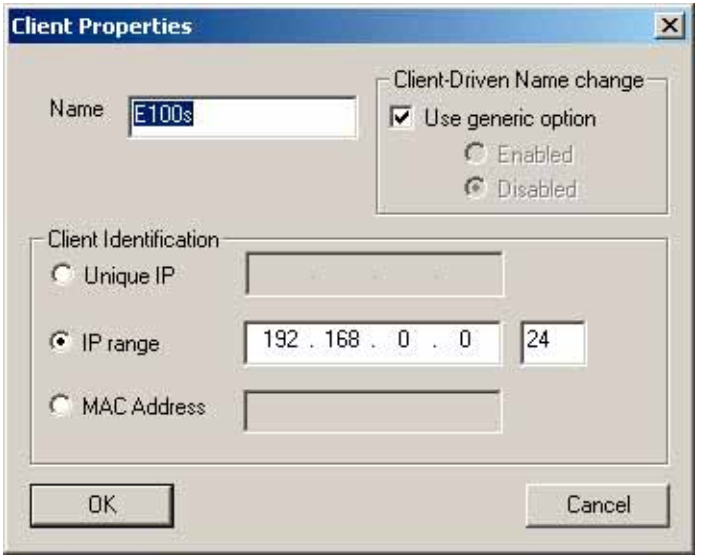
The **Help** menu enables you to display information about your version of the Neoware Image Manager Console.

Displaying & Changing Properties

The properties of a Computer, Group, or Volume can be displayed and changed either by right-clicking on its name and selecting **Properties** from the pop-up menu, or by selecting its name then display-

ing the **Edit** menu and selecting **Properties**. A **Properties** dialog is displayed when you create a Computer, Group or Volume.

Client Properties



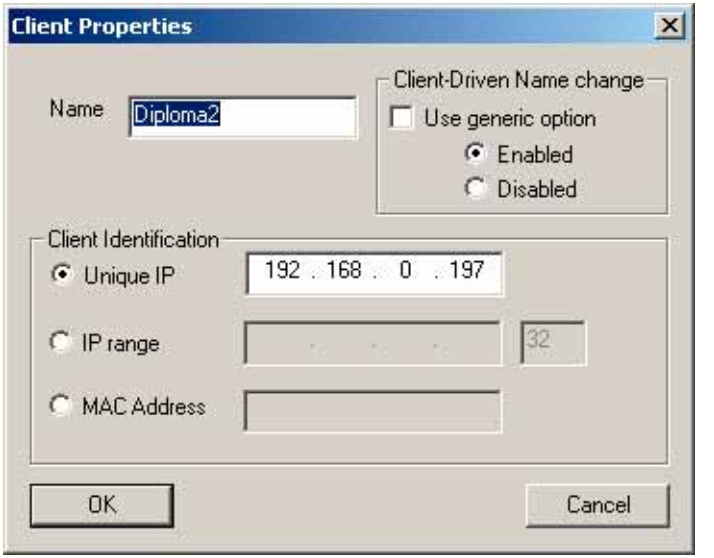
The **Client Properties** dialog enables you to specify the properties of a client Object. These properties contain the name assigned to the client object, whether this object is a collection of workstations or a subnet (or a single workstation), or an individual client identified by its IP address or MAC address.

Name

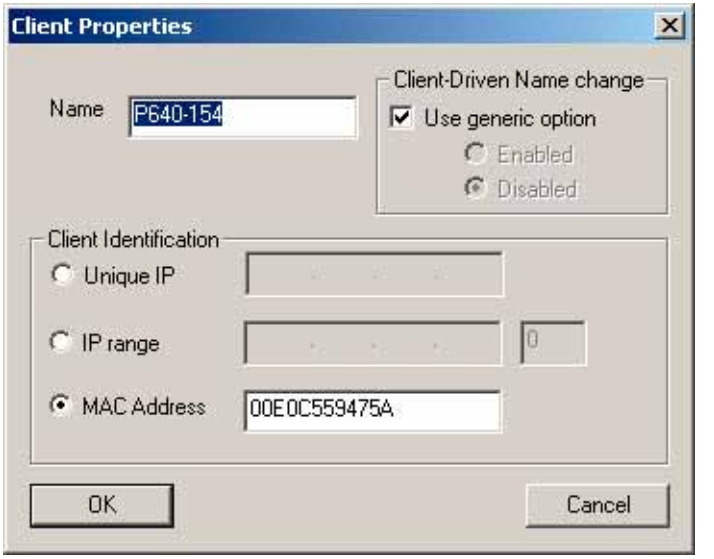
This field enables you to specify a name for the Client Object as it will appear in the Clients list.

Client Identification

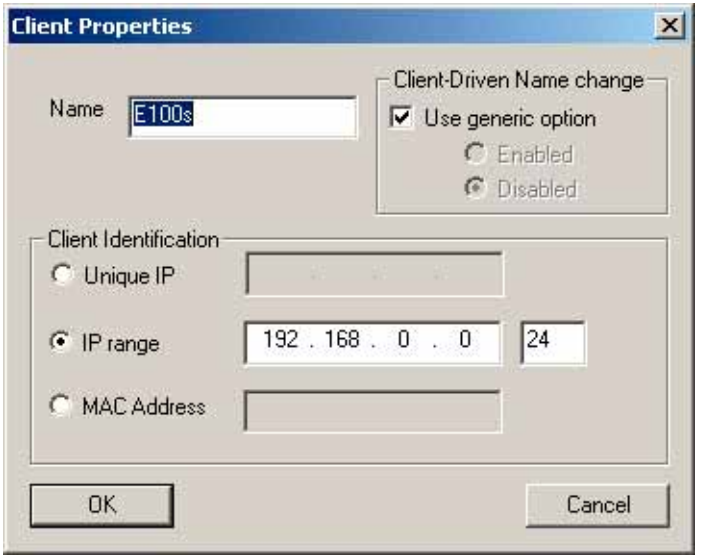
The Client Identification property specifies how Neoware Image Manager identifies the Client Object: either by specifying a single IP address,



or specifying a unique MAC Address,



or specifying an IP subnet.



When idenfified as a subnet, the identification is made of two fields. The IP address (address of the “network”) and the subnet mask.

Typical subnet masks are:

32 This is the subnet mask for a single IP address.
For example, 194.599.93.24/32 means a range of 1 IP address (a single client computer). When a client object identified by subnet has a subnet mask of 32, it is in fact a unique IP address and it will be treated accordingly.

24 254 IP addresses (a complete class C).
For example, 192.168.0.0/24 means all the IP addresses between 192.168.0.1 and 192.168.0.254.

16 65534 IP addresses (a complete class B).
For example, 172.16.0.0/16 means all the IP addresses between 172.16.0.0 and 172.16.254.254.

0 Is usually only used with IP address 0.0.0.0.
0.0.0.0/0 means all the IP addresses.

If several definitions exist that match the same client, the priorities are as follows (highest priority first):

1. MAC address,
2. Unique IP address (actually IP subnet with subnet mask of 32 bits),
3. IP subnet with subnet mask of 31 bits,
4. IP subnet with subnet mask of 30 bits,

...

33. IP subnet with subnet mask of 1 bit,
34. IP subnet with subnet mask of 0 bit (actually 0.0.0.0/0, the “everybody” group in the default `nvdd.conf` file).

It is recommended that you keep the "everybody" client object in order to define the “otherwise unknown clients”.

Client-Driven Name Change

Neoware Image Manager has the capability to retain individual client names, based on their MAC addresses, even when they booted in volatile mode. In particular, Neoware Image Manager server can record a name that changed so that the corresponding client will get the new name when it reboots, even if it boots in volatile mode. The feature, called “Client-Driven name change” can be enabled or disabled. In most cases, you do not want the users to be able to change a client name.

The Neoware Image Manager configuration file contains a parameter that specifies the default behavior. This parameter is available in the **Tools** > **Generic options** dialog (see later in this section).

If you would like a specific client object to be able to change and save the client name in the `nvdd` configuration file in the future, uncheck the **Use Generic Option** check box and select the **Enabled** option.

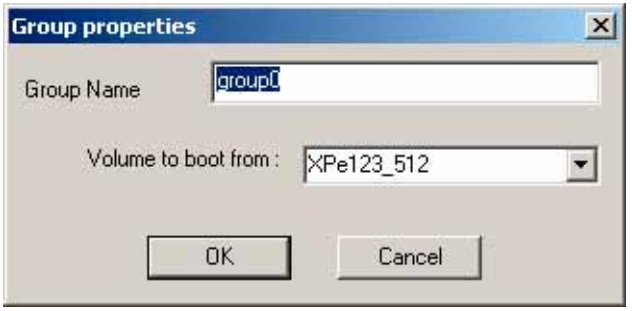
If you want to forbid this option, select **Disable**.

If you want this client to follow the default behaviour set in the **Generic Properties** dialog, check the **Use Generic Option** check box.

Note that when **Use Generic Option** is checked, the greyed options will reflect the value of the default options (either **Enabled** or **Disable**).

For more information on client naming, refer to the section "Client Naming" on page 233.

Group Properties

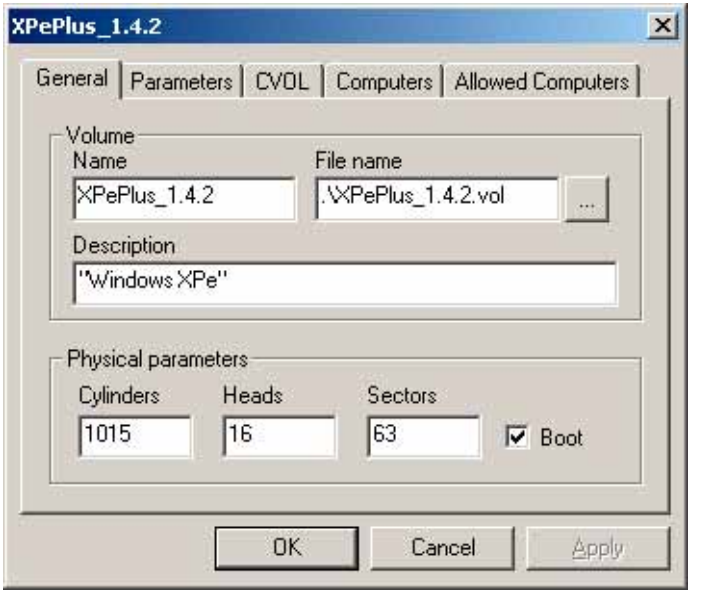


The Group Properties dialog specifies the name of a collection of computers (i.e. subnets). The volume that this group of computers use to boot from by default is specified by making a selection from the **Volume to boot from** list.

The boot volumes listed here are those that have the **Boot** option checked in their properties dialog and have been selected in the Volumes panel for the current group. Note that all the bootable volumes listed here will also be displayed on the client screen at boot time, enabling the user to choose the volume to boot from. This setting determines the volume that is used by default if the user does not make a selection within ten seconds.

If no bootable volumes are assigned to the currently selected group, the **Volume to boot from** list will be empty.

Volume Properties

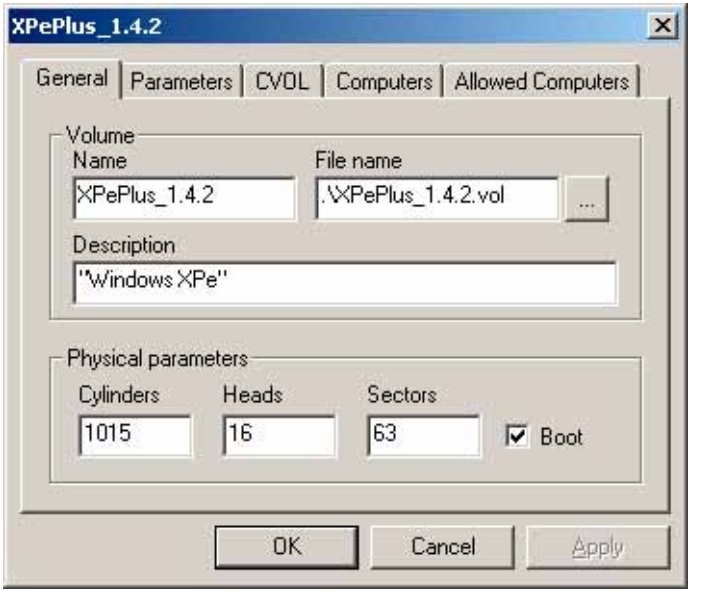


The **Volume Properties** dialog provides a range of options for defining a volume that can be accessed by clients. It is divided into several tabs, with the **General** tab shown by default. Refer to the section “Creating a Volume” on page 193 for details.

Creating a Volume

You can create a new volume either by right-clicking in the Volume panel and selecting **Create Volume** in the pop-up menu, or by displaying the **Edit** menu and selecting **Create** then **Volume**. A dialog consisting of several tabs is displayed. This dialog is also displayed when you view the **Properties** of a selected volume.

The General Tab



The **General** tab enables you to specify a name for the volume that will be used to identify it in the Console and also as a prefix for associated CVol files, and the physical parameters of the volume.

CAUTION: *You should not change the name of a volume currently in use by Neoware Image Manager client, nor should you change a volume name if there are CVol files related to this volume that you want to use. If you change the name of a volume, existing CVol files related to this volume will not be linked to the volume anymore. The*

names of the CVol files are directly derived from the related Volume name and changing this name while the volume is mounted by Neoware Image Manager client will crash the clients.

The Console will display a warning when you want to change an existing volume name

Specify the name of the hard disk image file to use in the **File name** box (click the **...** button to browse for it), or enter the complete or relative (to the directory where the NVDD server module is located) path and filename if it is not in the same directory as the NVDD server module.

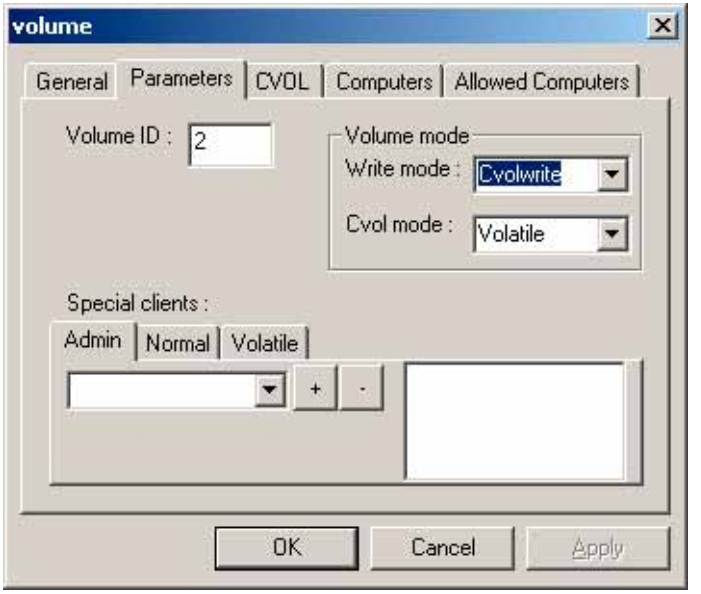
CAUTION:

- *You can change the File name of a volume currently in use by Neoware Image Manager client only when the new file is a copy of the old file. If this is not the case, changing the file name of a volume currently in use would be equivalent to hot-swapping the system disk of your clients with another system disk!*
- *If the volume is not currently mounted by Image Manager clients and you change the File name to an HDD image file that is not an exact copy of the previous one and there are existing CVol files associated with the volume, you must delete the CVol files (or make sure the client will all use Volatile mode) before the clients can actually mount the volume.*

The **Description** field enables you to provide a brief description of the volume which will be displayed on the client screen when it starts, when multi-boot is enabled (when the client can boot off various volumes).

The **Physical Parameters** options enable you to specify the "physical parameters" of the volume and whether it is used as a boot drive or as storage. The single-volume configuration file that Client Builder creates contains the parameters (especially geometry parameters) to be used with the corresponding volume.

The Parameters Tab

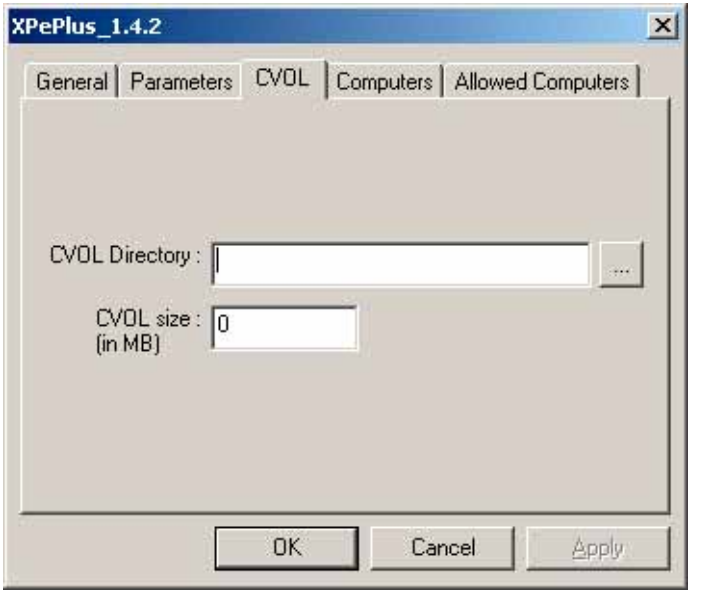


The **Parameters** tab enables you to specify the client writing mode for the volume and how it is shared.

The **Volume Mode** settings enable you to specify the standard writing mode to be used, while the **Special clients** options enable you to specify a different writing mode for individual clients. (For a description of the writing modes, refer to the section "Volume Write Modes" on page 82.) The clients listed in the **Special clients** mode tabs are defined in the Neoware Image Manager server configuration file. (Refer to the appropriate sections for details.)

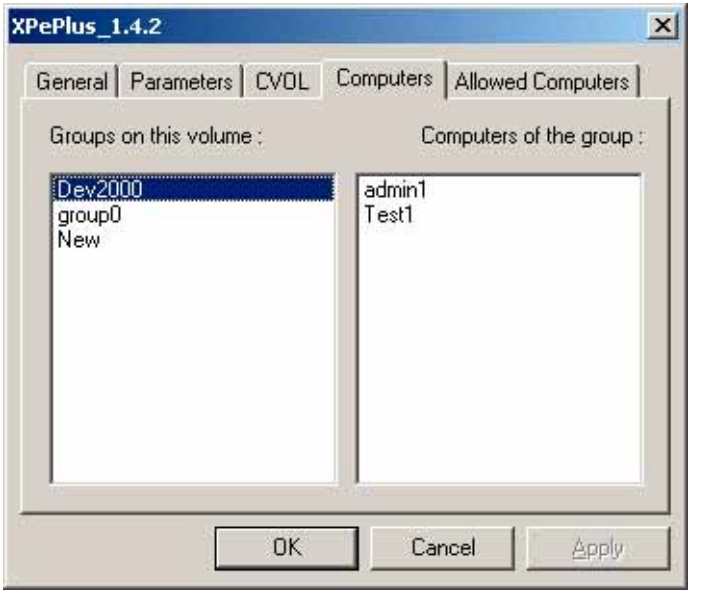
The **Volume ID** is the internal identification number that will be used for client/server communications. This number must be unique (one per volume). The numbers are usually generated automatically if the configuration file does not set them. The numbers are not generated automatically when a volume definition is imported from an existing configuration file (for instance, from a single-volume configuration file created by Client Builder).

The CVol Tab



The **CVOL** tab enables you to specify a different directory for this volume's CVol files if they are not to be stored in the general CVol directory (specified in the **General** tab of the **Generic Properties** dialog). You can also specify the maximum size that the CVol data file for this volume can grow to. Note that you can change this maximum size even when there are existing CVol files related to this volume, even if some have reached the current maximum size. All you would need to do would be to restart the server or reload the configuration file and, sometimes (when the clients are frozen because of "disk full" errors), reboot the clients.

The Computers tab

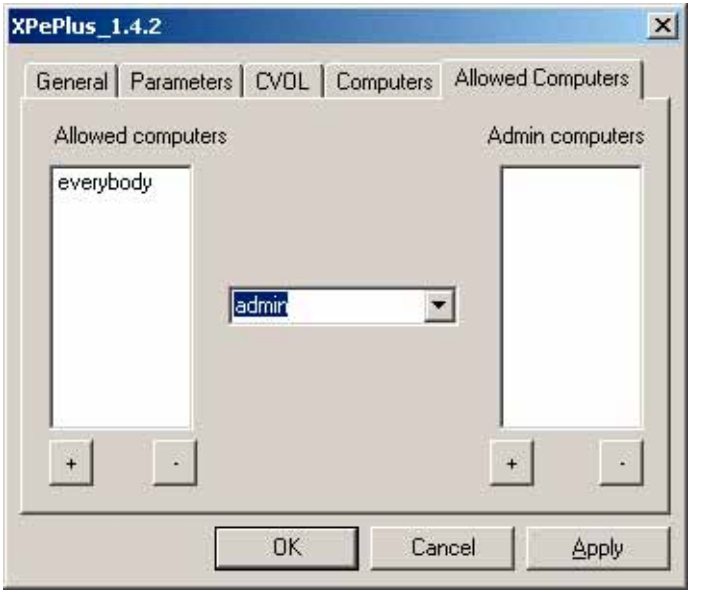


The **Computers** tab will display the names of all the computers that can share this volume. (This is not where you specify which computers share the volume.)

Double-clicking on a group or computer name will display the relevant **Properties** dialog.

We highly recommend that you set **Admin computers** according to your requirements and do not leave the client object "everybody" in this field. Only the actual clients allowed to perform administrative operations (changes in the image file itself) should be listed in this field.

The Allowed Computers Tab

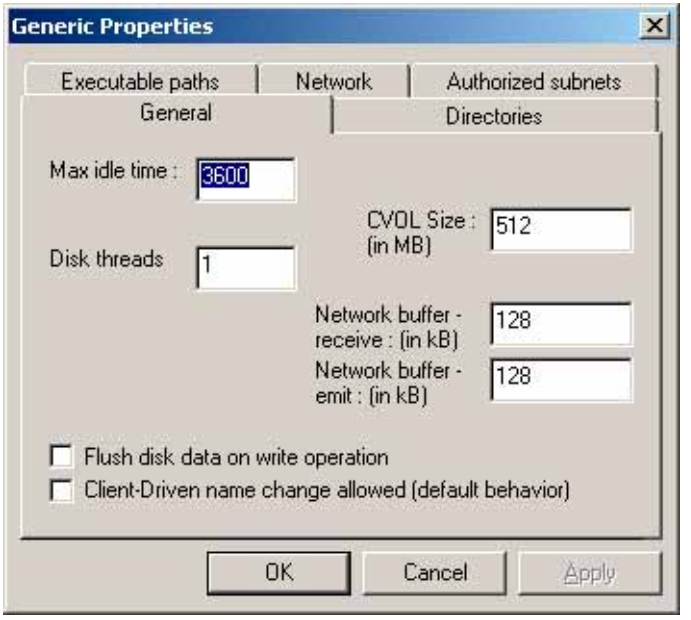


The **Allowed Computers** tab enables you to specify which computers or subnets are allowed to access this volume, and which computers or subnets are allowed in Admin mode.

To add a computer to the **Allowed computers** or **Admin computers** list, select the computer name in the central list box then click the **+** (plus) button under the relevant list box to add it to that list. To delete a computer from a list, just select its name then click the **-** (minus) button under the list.

Generic Options

The General Tab



The **General** tab enables you to specify settings that affect network access, the directory to use for client volumes, and the default maximum size of the CVol file and the default Client-Driven name change behaviour.

The **CVOL Size** setting specifies the maximum size that CVol data files can grow to.

Note that you can change this maximum size even when there are existing CVol files, even if some have reached the current maximum size. All you would need to do would be to restart the server or reload the configuration file and, sometimes (when the clients are frozen because of “disk full" errors), reboot the clients.

The **Flush disk data on write operation** option is used when you want to make 100% sure that when a client sends a request to write some data, it gets an acknowledgement that the write operation succeeded when the data have actually been written on the disk drive.

This option is usually set when you have a cluster of servers that use a shared storage.

Note: *This option has a negative impact on performance and is not recommended for servers that are not tailored for very fast disk operations.*

When used in "high-availability" environments, checking this option will make sure that if one of the servers in the cluster fails, no data will be lost: data that would have been sent to the server in write requests and that would not have been actually written to the disk would be considered by the client as non-written, then the client would re-send its write request.

When used in "high-availability" environments, unchecking this option could lead to situations when a client would have considered some data to have been written on the server's disk when actually this data could have not been transferred from the server's buffers to the disk. If the server fails while there are uncommitted data in its write buffer, another server would replace it (because there is a cluster of servers) but the data that have not been committed to the disk by the server that just failed would be lost, though the client would consider them as been written, resulting in potential data corruptions.

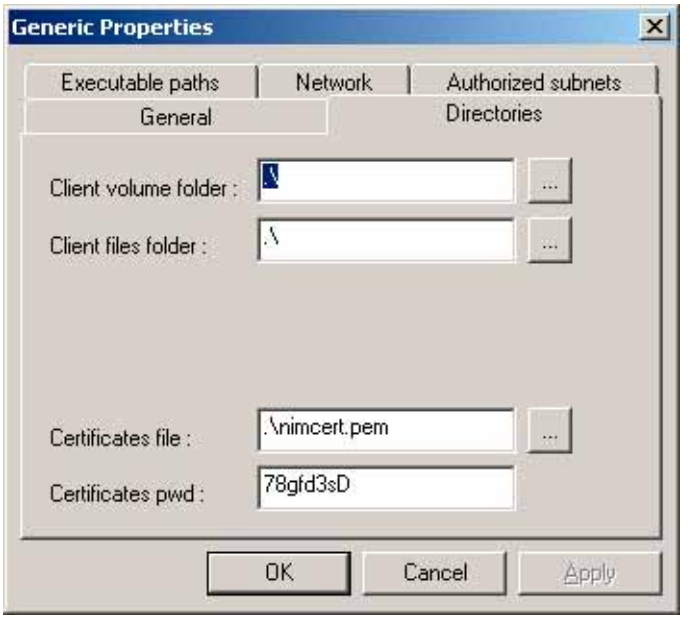
The setting of the **Client-Driven name change allowed (default behaviour)** option determines the default action of the NVDD server when a computer name is changed by a client during a session, and a specific Client-Driven name change property is not defined for the Client Object that contains that client. When this option is selected the server will store the new computer name in the `nvdd` configuration file by default so that it is reapplied the next time that client boots. When this option is not selected, the new computer name will not be stored, so when the client reboots it will reassert its original name. Note that the **Client Properties** dialog has a similar setting to

allow specific clients to override this general setting. For more information on client naming, refer to the section "Client Naming" on page 233.

Note: *If you disable the parameter* ***Client-Driven Name Change (default behavior)*** *and you enable Client-Driven Name Change for the Client Object "everybody" (IP range:0.0.0.0/0), this has the result that unknown clients (not identified by a unique MAC or IP address, belonging to "everybody" subnet), can store their name on the NVD server, but then this name cannot be changed unless the configuration file is modified so that the client has its Client-Driven Name Change property explicitly enabled.*

The other options in this dialog are described in the chapter "The NVDD Configuration File" on page 213.

The Directories Tab



The **Client volume folder** setting specifies the general directory where CVol files will be stored. Note that you can specify a different

directory for a volume's CVol files on the **CVOL** tab of the **Volume Properties** dialog.

The **Client files folder** setting specifies the root directory for file transfer. Files transferred by a client will be placed in a subdirectory within this directory. The name of each subdirectory will consist of the MAC address of the client initiating the file transfer. Any file transferred to or from the admin client (`nvddadmin`) must be based on this directory, or a subdirectory of it. If you used **Domain Credentials on NVDD Server**, the domain credentials for each client are also stored in this folder. Refer to the chapter "Adding Clients to Windows Domains" on page 147 for further details.

The **Client files folder** directory stores temporary files that the `nvdd` process creates, including a copy of the original server configuration file which the `nvdd` process actually works with. If the NVDD server experiences any problems, such as a power failure, temporary files that were in use will be stored in a subdirectory called `restored-files`, enabling an administrator to recover the data stored in them.

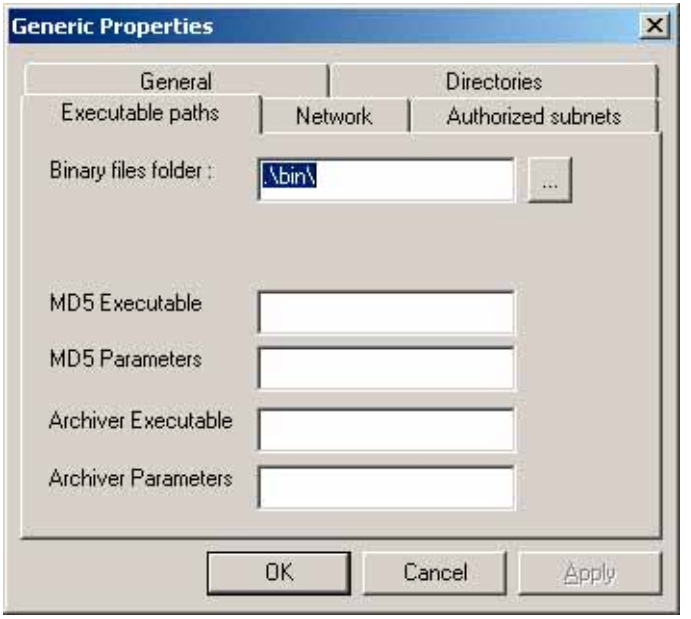
For more information on file transfer, refer to the appendix "File Transfer" on page 345.

The **Certificates file** setting specifies the name of the SSL certificate that the server is to use for admin connection.

The **Certificates pwd** setting specifies the password used to encrypt the certificate file (if any).

Note that even if SSL encryption is disabled in Neoware Image Manager, the certificate still has to be specified and valid.

The Executable Paths Tab



The **Binary files folder** setting specifies the path to the tools that can be launched by the server during a remote session from `nvddadmin`.

MD5 Executable and **Archiver Executable** enable you to specify different executable files to the default ones used for these operations.

MD5 Parameters and **Archiver Parameters** allow you to set custom parameters for the defined executables. These parameters will be taken into account ONLY if you provide executable names in the corresponding fields.

MD5 Executable default: `md5sum.exe` (Windows) or `md5sum` (Linux/BSD).

MD5 Parameters default: the only parameter given to the executable file will be the filename given by the administrator through `nvddadmin`. If **MD5 Parameters** is set, the parameters will be given first, followed by the filename. For example:

```
<md5_file> [<md5_params>] <filename>
```

Archiver Executable default: `gunzip.exe` (Windows) or `gunzip` (Linux/FreeBSD).

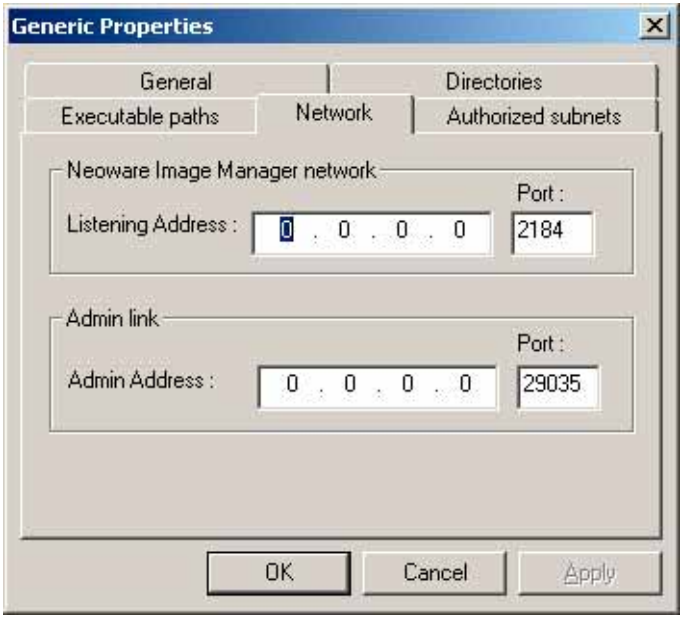
Archiver Parameters default: the only parameter given to the executable file will be the filename given by the administrator through `nvddadmin`. If **Archiver Parameters** is set, the parameters will be given first, followed by the filename. For example:

```
<unzip_file> [<unzip_params>] <filename>
```

Note that you can use batch file (`.bat` or `.cmd` under windows, shell scripts under Linux/FreeBSD) as the executable. This may be useful when using executable files that do not accept the file name as the last parameter.

These fields must contain the names of executable files names, which must reside in the folder indicated by **Binary files folder**. The appropriate permissions must be given to the executable files. Note that when run as a service under Windows, Neoware Image Manager runs by default under the authority of “SYSTEM” account

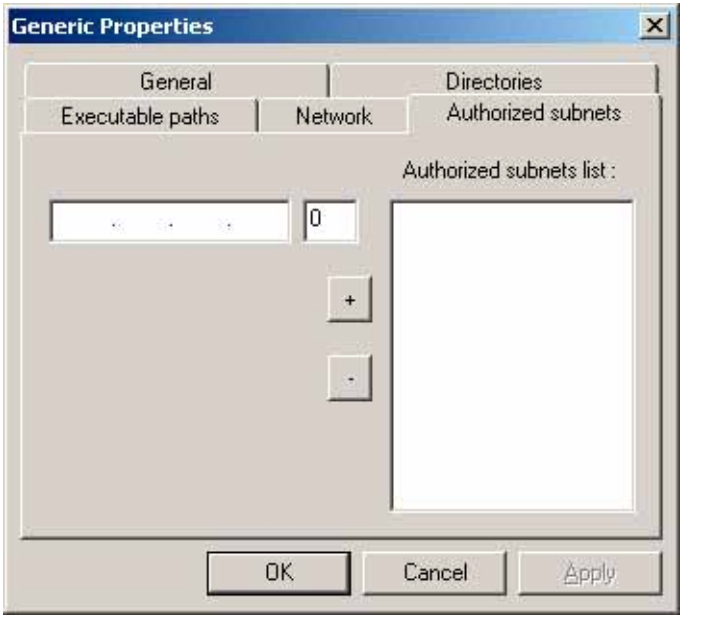
The Network Tab



The **Network** tab specifies the address and port to use for communicating with clients, and the Admin protocol address and port for communicating with the Image Manager server. Admin protocol is used by Client Builder to create the image file and by Neoware Image Manager Console to control running servers.

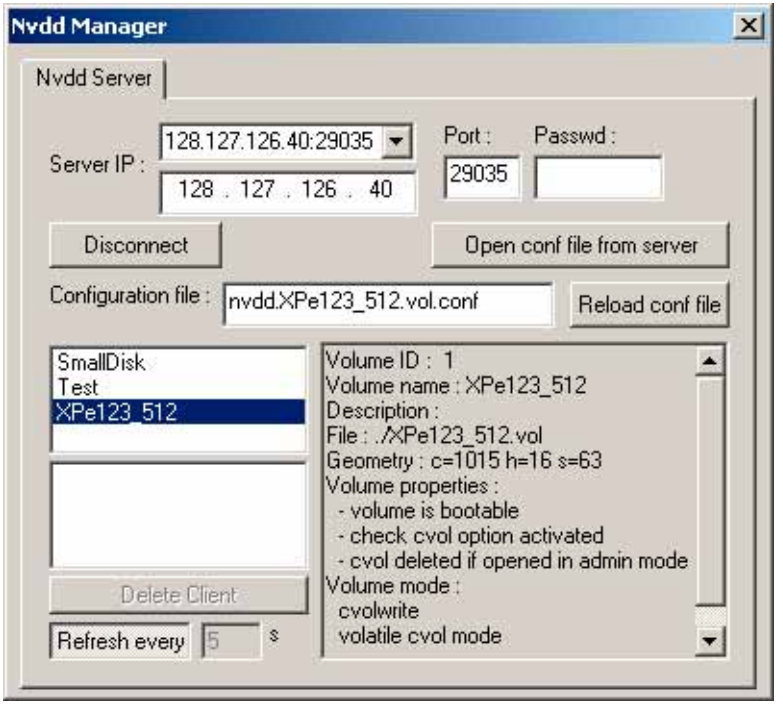
Specifying an IP address of 0.0.0.0 means all the IP addresses assigned to the server.

The Authorized Subnets Tab



The **Authorized subnets** tab is a security feature that allows you to configure the subnets the Image Manager server will accept. The server will accept requests from any IP address if no subnets are specified here.

The Nvdd Manager



One of the most useful features of the Console is the ability to manage running Image Manager servers.

Display the **Nvdd Manager** dialog by selecting **Nvdd Manager** in the **Tools** menu. This enables you to connect to and manage Image Manager servers directly.

To connect to a running Image Manager server, enter the server's IP address, port number (leave as **0** if using the default port number on the server side), and password if required, then click the **Connect** button. Note that the drop-down list contains the server addresses that have been used previously, so you can quickly select one of these.

When the Console runs on a computer that also runs the Neoware Image Manager server module, you can use **Nvdd Manager** and connect to IP address 127.0.0.1 (local host) or to any of the server's assigned IP addresses. This makes it possible to reload a modified configuration file, as long as the file has been opened by clicking the **Open conf file from server** button.

Note: *This method is the only one that can be used to actually modify a configuration file currently running. Editing the file (either with a text editor or with the console using* ***File > Open****) is not possible as the configuration file is locked.*

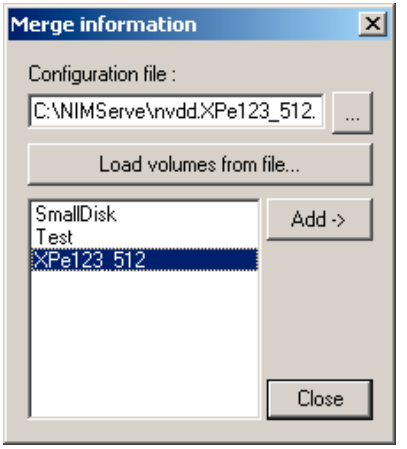
When communication has been established with the remote server, the two list boxes on the left side of the dialog will show the volumes shared by the server and the clients currently communicating with it. You can select volumes or clients to obtain detailed information on them.

You can force the deletion of a client by clicking the **Delete Client** button. *This will not remove the client* from the configuration, but stop communication with it - and remove any resource allocated to it. It may be useful to allow administrators to access CVol files.

The name of the configuration file currently being used by the remote server is displayed in the **Configuration file** field. You can edit this file within the **Nvdd Manager** dialog by clicking the **Open conf file from server** button. When you have finished, click the **Reload conf file** button to make the remote server take the changes into account. The configuration file must have been saved beforehand (using the **Save** command or button). When you click the **Reload conf file** button, the connection to the server is lost. You can click on **Connect** again when you want to reconnect to the server.

Clicking the **Refresh every** button will update the contents of the dialog that contains the refresh interval, otherwise the contents will be updated automatically after every number of seconds specified.

Merging Configuration Files



The Console enables you to import volume details stored in another configuration file, especially single-volume configuration files created using Client Builder. The merge command enables you to copy volume definitions from another configuration file into the current configuration file.

Display the **Merge Information** dialog by selecting **Merge conf file** in the **Tools** menu or by clicking the corresponding icon.

Select the desired **Configuration file** by using the **...** button to browse for it. Click the **Load volumes from file** button to list the names of the volumes defined in that configuration file.

Select the volume you want to copy to the current configuration file then click **Add**. The volume will appear in the **Console Volumes** list. Repeat for each volume you want to add.

You must make sure that the properties of each copied volume specify the location of the hard disk image file associated with the configuration file currently being modified. To do this, double-click on the name of the volume to display the **Volume Properties** dialog,

then change the path specified in **File name**, or browse to find the image file. Click **OK** to finish. Volume IDs for imported volumes may also have to be tuned manually so that they do not use an existing ID.

Password for Remote Administration

You can configure an NVDD server module so that a password is required in order to control it remotely using the Image Manager Console or Client Builder. This is achieved using the `NvddPasswd` utility.

The procedure is as follows:

1. Locate the file `NvddPasswd.exe`, usually in one of the following subdirectories:

   ```
   C:\Program Files\Neoware\Image_Manager_4.6\
   SERVER\Tools
   ```

   ```
   C:\Program Files\Neoware\Image_Manager_4.6\
   SERVER\WINDOWS\Tools
   ```

   ```
   C:\Program Files\Neoware\Image_Manager_4.6\
   SERVER\Linux\Static\Tools
   ```

   ```
   C:\Program Files\Neoware\Image_Manager_4.6\
   SERVER\Linux\Dynamic\Tools.
   ```

2. Copy `NvddPasswd.exe` (or `NvddPasswd` for Linux/FreeBSD servers) into the same directory as the `nvdd` server module.

3. Open a shell (command prompt) and key in `NvddPasswd.exe` (Windows) or `./NvddPasswd` (Linux/*BSD).

4. Type in the password to be used, press the **Return** key, then confirm the password by typing it again.

The `NvddPasswd` utility must be launched whenever the administrator wants to set or change a password that Neoware Image Manager Console users must enter when they want to control an NVDD server module remotely.

Note: *`NvddPasswd` can be used while `nvdd` is running. You do not need to restart `nvdd` for the new password to be taken into account for new connections.*

CHAPTER 17

The NVDD Configuration File

This chapter describes the nvdd configuration file and the settings that can be specified in it.

Introduction

The `nvdd` configuration file is used to define virtual hard disk volumes and specify which clients can access them. Every hard disk image that Client Builder creates will have an associated configuration file called `nvdd.<image filename>.conf`. When you install Neoware Image Manager it will provide you with a basic hard disk image file called `smalldisk.vol` and a configuration file called `nvdd.smalldisk.vol.conf`.

Whenever you build a hard disk image using Client Builder, it will automatically create a new configuration file called `nvdd.<image filename>.conf`. For example, if you create an image file called `XPe123.vol`, the configuration file for that image will be named `nvdd.XPe123.vol.conf`.

The Image Manager Console provides a graphical interface for editing an `nvdd` configuration file (see "The Image Manager Console" on page 181), or you can use any text editor to manually edit the file as described in this chapter.

The nvdd.smalldisk.vol.conf File

The `nvdd.smalldisk.vol.conf` file supplied in the Image Manager installation provides default configuration settings for the basic hard disk volume `smalldisk.vol` that is used as the foundation for creating hard disk images and volumes for clients to access.

The following shows the initial contents of the configuration file `nvdd.smalldisk.vol.conf`. These settings enable you to start using Image Manager to create images and volumes straight away.

```
address=0.0.0.0
port=2184
admin_addr=0.0.0.0
admin_port=29035

#authorized_subnets = 127.0.0.1/32, 192.168.0.0/24
authorized_subnets=


# client_volumes_dir is the directory where the client
# storage files are stored. The leading slash is needed.
# Note that you can not use backslashes (\) in the files
# and path names, you must use slash (/) instead.
# A sample for client_volume_dir being stored in
# D:\LANPC3\CVOL (Windows Style):
# client_volumes_dir = D:/LANPC3/CVOL/
# A sample for client_volume_dir being stored in
# /usr/local/lanpc3/cvol (Linux/Unix Style):
# client_volumes_dir = /usr/local/lanpc3/cvol/
client_volumes_dir=./


max_idle_time=3600


# sectors_map_size is the max number of sectors that
# can be stored in a client storage file (aka write
# cache file located on the server)
# One sector = 512Bytes = 0.5KB. 1048576 sectors = 512MB
sectors_map_size=1048576
```

```
disk_threads=1
recv_buf=131072
send_buf=131072

client_files_dir=./

bin_directory=./tools

certificate_file=./nimcert.pem

certificate_passwd=78gfd3sD


#
# USERS definitions
#
users=everybody, admin

everybody.subnets=0.0.0.0/0
admin.subnets=127.0.0.1/32

#
# VOLUME definitions
#
#volumes = vol0, vol1
volumes=SmallDisk

SmallDisk.id=1
SmallDisk.file=smalldisk.vol
SmallDisk.desc=Small 8MB Virtual Volume
SmallDisk.cylinders=1
SmallDisk.heads=255
SmallDisk.sectors=63
SmallDisk.floppy=false
SmallDisk.boot_device=false
SmallDisk.check_cvol=true
SmallDisk.no_admin_cvol=true
SmallDisk.write_mode=cvolwrite
SmallDisk.cvol_mode=volatile
SmallDisk.sectors_map_size=0
SmallDisk.client_volumes_dir=
SmallDisk.cache_size=0
SmallDisk.type=0
```

```
SmallDisk.users=admin, everybody
SmallDisk.unicast_users=admin, everybody
SmallDisk.admin_users=admin, everybody
SmallDisk.admin_mode_users=
SmallDisk.normal_mode_users=
SmallDisk.volatile_mode_users=

#
# GROUP definitions
#
groups=group0

#group0.vols = vol0, vol1
group0.vols=SmallDisk
group0.unicast=true

group0.read_only=false
group0.users=everybody, admin
```

Configuration File Settings

The following configuration file setting descriptions generally follow the order shown in the example `nvdd.smalldisk.vol.conf` file shown in the previous section.

Comments can be specified in the configuration file by beginning the line with the # character.

Caution: *Neoware Image Manager will erase existing comments when it modifies a configuration file.*

An example of a configuration file that supports multiple volumes can be found at the end of this chapter.

IP Addresses & Port Numbers

`address`

(optional – default: `0.0.0.0`)

Specifies the IP address used by the `nvdd` server for NVD (virtual HDD related) communications. Set this parameter if your server has several NICs or IP addresses.

`port`

(optional – default: `2184`)

Specifies the port number used by the `nvdd` server.

`admin_addr`

(optional – default: same as `address`)

Specifies the IP address that `nvdd` must use for administration purposes (NVDDAdmin protocol). Useful if the server contains multiple network cards.

`admin_port`

(optional – default: `29035`)

Specifies the port number used by the administration interface.

`authorized_subnets`

(optional – default: all subnets)

If this setting is present, `nvdd` will deny access to clients whose IP addresses do not match the comma-separated list of subnets.

A subnet definition is of the form: `a.b.c.d[/bits|:netmask]` where `a`, `b`, `c`, and `d` must be fully specified.

Timing

`max_idle_time`

(optional – default: `120`)

Clients that have not communicated with `nvdd` during this time (in seconds) will be automatically deleted.

Note that contexts are saved in CVol files, allowing clients to communicate with the server again without any problems.

Directory for Client Volumes

`client_volumes_dir=./`

This specifies the directory where client CVol files are stored for all volumes in this configuration file, unless overridden by the same command used in a volume definition. The trailing slash is required. Note that you can not use backslashes (\) in the file and path names, you must use slash (/) instead.

Example for client CVol files being stored in `D:\LANPC3\CVOL` (Windows format):

```
client_volumes_dir = D:/LANPC3/CVOL/
```

Example for client CVol files being stored in `/usr/local/lanpc3/cvol` (Linux/Unix format):

```
client_volumes_dir = /usr/local/lanpc3/cvol/
client_volumes_dir=./
```

To specify different CVol directories for individual volumes, precede the command with the volume name in the relevant volume definition. For example:

```
testdisk.client_volumes_dir = F:/LANPC3/CVOL/
```

Directories for File Transfer

`client_files_dir = ./files/`

This option specifies the root directory for file transfer.

Files transferred by a client will be placed in a subdirectory within this directory. The name of each subdirectory will consist of the MAC address of the client initiating the file transfer.

Any file transferred to or from the admin client (`nvddadmin`) must be based on this directory, or a subdirectory of it.

When NeoDomain has been run to enable Domain Credentials on Neoware Image Manager Server, Domain Credentials are stored in these subdirectories, in a file called `NeoDomSO`.

The directory specified by the parameter `client_files_dir` also stores temporary files that the `nvdd` process creates, including a copy of the original server configuration file which the `nvdd` process actually works with. If the NVDD server experiences any problems, such as a power failure, temporary files that were in use will be stored in a subdirectory called `restoredfiles`, enabling an administrator to recover the data stored in them.

For more information on file transfer and the directories used, refer to the appendix “File Transfer” on page 345.

Directory for Binaries

`Bin_directory = ./tools/`

This option specifies the path to the tools that can be launched by the server during a remote session from `nvddadmin`.

`Md5_file = [<filename>]`

(optional – default: `md5sum.exe` (Windows) or `md5sum` (Linux/BSD)

This specifies the name of the executable file the server is to use when it receives an "MD5" command from `nvddadmin`. The specified executable file will be used instead of the default `md5sum.exe` (Windows) or `md5sum` (Linux/BSD).

The executable file MUST be placed in the directory pointed to by `bin_directory`.

`Md5_params = [<params>]`

(optional)

If `md5_file` is set, this option is used to give the executable file its command line.

By default, the only parameter given to the executable file will be the filename given by the administrator through `nvddadmin`. If `md5_params` is set, the parameters will be given first, followed by the filename. For example:

`<md5_file> [<md5_params>] <filename>`

`unzip_file = <filename>`

(optional – default: `gunzip.exe` (Windows) or `gunzip` (Linux/BSD)

This provides the name of the executable file the server is to use when it receives an "UNZIP" command from `nvddadmin`. The specified executable file will be used instead of the default `gunzip.exe` (Windows) or `gunzip` (Linux/BSD).

This executable MUST be placed in the directory pointed to by `bin_directory`.

`unzip_params = <params>`

(optional)

If `unzip_file` is set, this option will be used to give the executable file its command line.

By default, the only parameter given to the executable file will be the filename given by the administrator through `nvddadmin`. If `unzip_params` is set, the parameters will be given first, followed by the filename. For example:

`<unzip_file> [<unzip_params>] <filename>`

Certificate File

`certificate_file=./Certificates/cacert.pem`

This specifies the name of the SSL certificate that the server is to use for admin connection. Although SSL encryption is disabled in Neoware Image Manager 4.5, the certificate file must still be present and the parameter that specifies its path must be correctly set.

`certificate_passwd=[<xxx>]`

(optional)

This gives the server the password used to encrypt the certificate file (if any).

Maximum Size of CVol Files

`sectors_map_size`

(optional – default: `512`)

This specifies the maximum number of sectors that can be stored in each client CVol write cache (data) file for all volumes defined by this configuration file, unless overridden by the same command used in a volume definition. One sector = 512Bytes = 0.5KB. 1048576 sectors = 512MB.

Warning: *Once you have changed this value, you need to restart nvdd server or reload the configuration file in order for the new setting to be taken into account.*

To specify different sizes for individual volumes, precede the command with the volume name in the volume definition. For example:

`smalldisk.sectors_map_size=16128`

For small volumes, administrators can set the sector map size to be exactly the same number of sectors in the logical volume. This will enable the volume to be completely customised on a per-volume basis.

If the CVol file becomes full and the sector map size for a volume is less than the total number of sectors in the volume, Image Manager will issue a Disk Full error message. The Windows operating system will not crash and you can usually shut it down (though the user may

have to respond to many Delayed Write Failed messages by clicking the **OK** button). You can then increase the sector map size value so that when the server is restarted the client can continue its write operations.

If the CVol file becomes full and the sector map size for a volume is the same as the total number of sectors in the volume, a "Disk Full" or "Delayed Write Failed" error message will be issued. In this case, just erase some files from the mounted volume, on the client side, to make some sectors in the CVol file considered as available by the Windows operating system running on the client.

Computer Name Change Default

`default_save_name=[true¦false]`

(optional – default: `false`)

The setting of this option determines the default behaviour of the server when a computer changes its name during a session.

If `true`, the new name for the computer will be saved in the configuration file and will be restored to the computer the next time it boots. If `false`, the change is lost, and the computer will keep its previous name.

For more information on client naming, refer to the section “Client Naming” on page 233.

Flush Disk Buffers on Write

`do_flush_on_write=[true¦false]`

(optional – default: `false`)

The setting of this option determines the default behaviour of the server when a client computer sends a write request.

If set to `true`, the server will send a write acknowledgement to the client only after data has actually been written on the physical storage. Therefore, if there are uncommitted data in the server’s write buffer and the server fails before committing this data, the client will not consider them written and will resend its write request.

This option is intended to be used in a high-availability environment when there are several servers that can write to the same shared storage.

Number of Processing Units

`disk_thread`

(optional – default: `1`)

Specifies the number of processing units dedicated to disk operations. This value can be tuned depending on the server resources to enhance performance.

It is useless setting this parameter to a value exceeding the maximum number of clients that access the server at the same time.

It is usually useless to set this parameter to a number greater than the the number of CPU in your server added to the number of physical hard disk drives that are accessible in parallel at the same time.

If you have only one HDD in a single CPU server, this value should be set to 1.

Buffer Size

`recv_buf`

Specifies the size, in bytes, of the buffer for receiving network data.

`send_buf`

Specifies the size, in bytes, of the buffer for data to be transmitted on the network.

User Definitions

`users`

Comma separated list of valid user definitions. User definitions are actually client objects and are determined by their IP address range or MAC address. For example:

```
users=everybody, admin
```

`<user>.subnets`

Defines a comma separated list of subnets.

A station is identified by its IP address and given the name of the last matching subnet of different client (named “users”) definitions. More details about IP addresses notation with slash can be found here:

`http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-address.html`

Note that if the subnets restrict the identification to a unique computer (bits=32), then the client will be able to receive its name from the NVDD server.

Client MAC Address *<user>*`.MAC=`*<MAC_address>*

This specifies the MAC address of a client. This client will be uniquely defined in the configuration file and will be able to receive its name from the NVDD server.

Note that a client can still be identified by an IP subnet or IP address (in fact an IP subnet with a subnet mask of 32 bits). If several definitions exist that match the same client, the priorities are as follows (highest priority first):

1 MAC address,

2 Unique IP address (actually IP subnet with subnet mask of 32 bits),

3 IP subnet with subnet mask of 31 bits,

4 IP subnet with subnet mask of 30 bits,

...

33 IP subnet with subnet mask of 1 bit,

34 IP subnet with subnet mask of 0 bit (actually 0.0.0.0/0, the “everybody” group in the `nvdd.conf` file).

It is recommended that you keep the "everybody" client object in order to define the "otherwise unknown clients".

Computer Name Change

`<user>.save_name=[true¦false]`

This option defines the behavior of the server when the client changes its name during a session. If it is not specified, it defaults to the global value `default_save_name`.

When defined for a subnet, this parameter is applied to all the clients that belong to this subnet and do not belong to a more precise subnet or are not defined by MAC address.

If `save_name` is `true`, the new client's name will be saved in the configuration file. Otherwise the change is lost and the computer keeps its previous name at next reboot.

For more information on client naming, refer to the section “Client Naming” on page 233.

Volume Definitions

`volumes`

Comma separated list of valid volumes definitions. Please note that at least one volume must be present. For example:

```
volumes=SmallDisk, XPe512, TestDisk
```

Each volume has to be defined with details such as file, cylinders, heads and sectors, etc. using the following commands.

Volume ID & Name

`<volume_name>.id`

Assigns a unique ID number for this volume.

`<volume_name>.file`

Specifies the name of the hard disk image file to use. For example:

```
SmallDisk.file=smalldisk.vol
```

`<volume_name>.desc`

(optional)

Provides a description of the volume. This text is displayed in the client’s boot menu when there is a choice of bootable volumes to

choose from (i.e. if several bootable volumes are available to this client).

For example:

```
disk0.desc=Windows XP sp2 (Back Office)
```

Volume Geometry

The following parameters are created by Client Builder when it creates the image file and associated configuration file.

`<volume_name>.cylinders`

Specifies the number of cylinders for the virtual disk.

`<volume_name>.heads`

Specifies the number of heads for the virtual disk.

`<volume_name>.sectors`

Specifies the number of sectors for the virtual disk.

Volume Type

`<volume_name>.floppy`

(optional – default: `false`)

Specifies if this volume is a floppy image. Unit letters at DOS/BIOS level depend on this. Value: `true` or `false`.

`<volume_name>.boot_device`

(optional – default: `false`)

Specifies if this volume is a boot device. Value: `true` or `false`.

Refer to the section “Enabling Client MultiBoot” on page 235 for details on how to specify a choice of volumes for a client to boot from.

`<volume_name>.type`

This parameter is now obsolete and performs no function. It is retained only for compatibility with earlier versions of Neoware Image Manager.

Volume Integrity

<*volume_name*>.check_cvol

(optional – default: false)

This parameter is used to make nvdd check the integrity of CVol files before opening them. Integrity is checked by the comparing the CVol file date with the image file date. If a CVol file is older than the image file it refers to, this means that modifications has been made on the image and the CVol file has not been updated. In this case, if check_cvol=true, the CVol file is deleted and reconstructed. If a reference CVol file exists for this client, it is also deleted (see cvol_mode for more information on reference CVols). This check is made when a client boots, before the client actually mounts the corresponding volume, and only for the CVol file corresponding to this client and that volume.

If this parameter is not specified, the default value is false.

When this parameter is enabled, it is then required that the server's date is correctly set.

Volume Write Mode

<*volume_name*>.write_mode=[admin¦cvolwrite]
<*volume_name*>.cvol_mode=[normal¦volatile¦persistent]

These commands specify the default write mode for a volume.

If the write mode is set to admin, and the following command is specified:

<*volume_name*>.no_admin_cvol=true

the CVol file relating to the client mounting the volume will be deleted before the client actually boots. All write operations will then be made on the hard disk image file itself. The default setting for <*volume_name*>.no_admin_cvol is false.

If the write mode is set to `cvolwrite`, then the `cvol_mode` command specifies the submode.

You can also specify different write modes for specific clients using the same volume, so the default write mode is ignored. The following commands would be used to indicate which clients are to use which mode:

```
<vol_name>.admin_mode_users=<comma separated clients>
<vol_name>.normal_mode_users=<comma separated clients>
#(CVolWrite/Normal)
<vol_name>.volatile_mode_users=<comma separated clients>
#(CVolWrite/Volatile)
```

If the writing mode is set to CVol write and the submode is normal, the following command will cause the Image Manager server to automatically check if the hard disk image has changed. If it has, then the CVol files will be emptied:

```
<volume_name>.check_cvol=true
```

(The check is made on the file dates.)

Normal CVolwrite Mode

When CVolwrite Normal mode is specified, write operations are kept in the CVol files when the corresponding client is booting.

Volatile CVolwrite Mode

If CVolwrite Volatile mode is specified, when a client is booting, the corresponding CVol file is emptied. Write operations are then not kept when a client is rebooted and the system configuration is always in the same state after a reboot. All changes to the volume, such as creating new files or folders, installing applications, modifying the system settings, do not survive a reboot.

Persistent CVolwrite Mode

If CVolwrite Persistent mode is specified, when a client is booting, the corresponding CVol file is replaced by reference CVol files that

will have the same name plus the extension `.ref` for the header, and `.ref.dat` for the data file. If this reference CVol does not exist, it will be copied from the existing CVol file for this client. This means that the first time a volume is opened by a client in Persistent mode, the reference CVol file is automatically copied from the existing CVol file. Each time after that, the CVol file is replaced by this copy when the client boots, ensuring that the client boots a well known configuration and retains all the information contained in the first CVol file (for instance, Windows XP activation data for this client).

The following example is a detailed description of what happens when `vol0.cvol_mode = persistent` and a client with the MAC address `00E0C554E700` boots and mounts the volume named `vol0`:

Case 1: If a file named `vol0@00E0C554E700.ref` exists in the folder where CVol files are stored, the file `vol0@00E0C554E700.ref` is copied to `vol0@00E0C554E700` before vol0 is actually mounted by the client. The same is done for the data file `vol0@00E0C554E700.ref.dat`, copied to `vol0@00E0C554E700.dat`

So the files `vol0@00E0C554E700.ref` and `vol0@00E0C554E700.ref.dat` replace `vol0` CVol files for the client `00E0C554E700`. In this case, the presence of a file named `vol0@00E0C554E700` does not make any difference in `nvdd` behavior.

Case 2: If a file named `vol0@00E0C554E700.ref` does not exist in the folder where CVol files are stored but a file named `vol0@00E0C554E700` does exist in this folder, the file `vol0@00E0C554E700` is copied to `vol0@00E0C554E700.ref` and the file `vol0@00E0C554E700.dat is copied to vol0@00E0C554E700.ref.dat` before `vol0` is actually mounted by the client. Those files then become the reference CVol files for client `00E0C554E700`. Each time it is rebooted afterwards, the client mounts `vol0` volume with a copy of `vol0@00E0C554E700.ref` and `vol0@00E0C554E700.ref.dat` as its CVol files.

Case 3: If the files named `vol0@00E0C554E700.ref` and `vol0@00E0C554E700` do not exist in the folder where CVol files are stored, then a file named `vol0@00E0C554E700` will be created in the

CVol file folder and will be treated as a normal CVol. Note that in this case, when the client reboots, the reference CVol file will be created from the current CVol file for this client (file `vol0@00E0C554E700`) as described in Case 2 above.

In order to create a reference CVol file, you can either copy an existing CVol file to the corresponding reference CVol file, or you can make sure that no CVol file exists for a particular client, set the `cvol_mode` parameter for the volume to `persistent`, boot the client, perform the needed customization tasks (activate Windows XP for instance), and reboot the client. The reference CVol file will then be created automatically.

You can also set the `cvol_mode` parameter for the volume to `normal`, make all the required modifications until your CVol suits your needs, including reboot if required, and then change the mode to `persistent`, making this CVol the reference for all subsequent reboots.

Directory for CVol Files

`<volume_name>.client_volumes_dir`

(optional)

If defined, this will be the folder used to store the CVol files for this volume.

If not defined, the CVol files will be stored at the normal folder (see the section “Directory for Client Volumes” on page 218).

Cache Size

`<volume_name>.cache_size`

(optional)

This parameter specifies the size, in number of sectors, of the server cache for the specified volume. The value must be a signed integer (only positive values are valid). Value `0` means no cache and this is recommended on systems with good disk cache (Windows Servers, Linux/*BSD Servers).

This option is currently unsupported and is present only for compatibility with earlier versions of Neoware Image Manager.

Allowed Clients

<*volume_name*>.users

Comma separated list of clients allowed to access this volume.

<*volume_name*>.admin_users

(optional)

Comma separated list of clients allowed to access this volume as administrators. Note that only one administrator client is allowed at the same time. When an administrator is accessing the disk, all other clients are refused. An administrator client cannot access specified volumes when some other (non-Admin) clients are still present.

<*volume_name*>.read_only_users

(optional)

Comma separated list of clients allowed to access this volume in read only mode. See also group.read_only.

<*volume_name*>.unicast_users

Comma separated list of users allowed to access this volume in unicast. See also group.unicast.

Group Definitions

groups

This is a comma separated list of group definitions. A group is used at initialization time to determine which clients can access the shared drives. Depending on the client user name (see users), nvdd will tell the client which volumes it should mount and assign specific modes. Please note that this information is only general, real authentication is ruled at volume level.

<*group_name*>.vols

This is a comma separated list of volume names that stations belonging to the group should access.

`<group_name>.unicast`

(optional – default: `false`)

This specifies if the stations should mount volumes in unicast or not. Values: `true` or `false`.

`<group_name>.read_only`

(optional – default: `false`)

This specifies if the station should mount volumes in read only mode or not. If so, all write requests will be discarded.

`<group_name>.users`

This is a comma separated list of users in group. The best matching user subnet is chosen to specify if a client uses the group parameters.

`<group_name>.wrappers`

(optional)

This is a comma separated list of wrapper definitions in the form: `a:b`, where a is the origin unit and b is the mapping unit. `a` or `b` can be specified in using 0x prefix (specifying hexadecimal) or 0 prefix (specifying octal) instead of the default decimal base.

This option is currently unsupported and is present only for compatibility with earlier versions of Neoware Image Manager.

Client Naming

Neoware Image Manager uses several methods to assign names to clients. You can either specify the name of a client directly in the `nvdd` configuration file using the NVD protocol (highest priority), or if no name is specified one will be assigned either based on DHCP option 12 (client host name) or, if no DHCP option 12 was set for this client, a name consisting of the letter H + the client MAC address.

This name is used as the NetBIOS client name (Windows Client Name) and also as the "Internet Host Name" (TCP/IP name). Both names are usually the same in Windows 2000, XP and 2003.

Setting Client Name using NVD Protocol

The following example `nvdd` configuration file entries show the various methods of specifying client names. The highlighted entries show the client name set directly using the NVD protocol.

```
User=everybody, office, pc-john, pc-paul

everybody.subnets=0.0.0.0/0
office.subnets=192.168.2.0/24
pc-john.mac=00015474AB1B
pc-paul.subnets=192.168.15.64/32
```

The client with MAC address 00015474AB1B will be named PC-JOHN (Windows computer name).

The client with IP address 192.168.15.64 will be named PC-PAUL.

The clients in the subnet 192.168.2.0 will be named according to the DHCP option #12 for each client or, if no DHCP option #12 exists for such a client, it will be named `H<client_MAC_address>`

Updating Client Name from Client

When a client name has been set using the NVD protocol, it can be updated from the client side. At shutdown time the client sends a message to the NVDD server in which the client's name is embedded. If the client name has changed or does not exist, the NVDD server can then record this name in the `nvdd` configuration file. This feature can be disabled using the `save_name` property of the client object so that unauthorized clients cannot actually change their name.

If you set the default global property `default_save_name` to `false` and the property `everybody.save_name` to `true`, this has the result that unknown clients (not identified by a unique MAC or IP address, belonging to "everybody" subnet), can store their name on the NVD server, but then this name cannot be changed unless the configuration file is modified so that the client has its `save_name` property set to `true`.

If existing clients (identified by a unique IP or MAC address) do not have their own `save_name` property, their default behaviour is ruled by the value of the global parameter `default_save_name`.

For example, if the client name has changed (using a Windows System applet or by manipulating the registry), and if the property `save_name` is set to `true` for the client (or IP range if the client is not uniquely defined), the new name can be stored on the server side so that it will be used at next boot (standard Windows behaviour). This will also be the case if the global parameter `default_save_name` is set to true and the client has a unique definition but no `save_name` property.

Note: *The property `save_name` is set to `false` by default.*

The property is NOT propagated. This means that, though `everybody.save_name` is set to `true`, a client that does not have the property `save_name` explicitly set to `true` will not be able to change its name from the client side (even if that client is a member of the group `everybody`), unless the global parameter `default_save_name` is set to `true`.

Enabling Client MultiBoot

Neoware Image Manager provides a MultiBoot feature. When two or more bootable volumes are associated with a client, the client will display the descriptions of these volumes so that the user can select the one to boot from. If no selection is made within 10 seconds, the client will boot using the default volume.

The names of the boot volumes are specified together with any other volumes using the parameter `<group_name>.vols`, where `<group_name>` is replaced by the actual group name that the client belongs to. This is followed by a comma-delimited list of volume names. For example:

```
AsusGroup.vols=WinXP, Win2K
```

At boot time, `mPXELdr` gets the list of bootable volumes for the client it is run on and displays a menu similar to the following:

```
Neoware Primary BootStrap Loader
1.5.0.9 (NVD protocol v3.0)
Copyright 2000-2006 Neoware Systems
All rights reserved
Available RAM (KB): 556
No .ini file (or 'NVDServers' key invalid/not found).

Client Config:
Subnet :  255.255.255.  0
Gateway : 192.168.0.1
MAC :     00 :E0 :C5 :59 :32 :FA
IP :      192.168.  0.155

Trying to connect to nvd server :
IP : 192.168  0. 10   PORT :  2184
MAC : 00:16:36:07:62:CF

1) HD, Windows XP Pro
2) HD, Windows 2000 Pro
```

The user then keys in the number of the volume to boot from.

mPXELdr gets the parameter <*volume_name*>.desc of each bootable volume. mPXELdr displays this description after the number assigned to the corresponding volume. If there is no <*volume_name*>.desc parameter for a specific volume, mPXELdr will not not display anything after HD,.

The first volume in the list is assigned the number 1, the second volume is assigned number 2 etc. The user can press 1 to boot from volume number 1, 2 to boot from volume number 2, etc. After a timeout of 10 seconds, if no volume was chosen, mPXELdr will start booting from volume number 1.

Note:

- Only bootable volumes (volumes for which the parameter <*volume_name*>.boot_device is set to true, which corresponds to the "boot" option in the **General** tab of **Volume properties** in the Neoware Image Manager Console) are displayed as boot menu choices.
- The volumes in the <*group_name*>.vols list that are not bootable are mounted as extra volumes under Windows (assigned to the drive letters D:, E:, etc. for instance).
- Only one bootable volume is mounted by Windows. This is the volume that was chosen as the boot volume at boot time. The other bootable volumes are ignored.
- The default boot volume (Virtual HD #1) is the first volume name listed by <*group_name*>.vols.

Tip:

If you want to mount a volume that is usually a bootable volume as an extra volume, you can change the <*volume_name*>.boot_device parameter for that volume to false, then specify the name of this volume in the <*group_name*>.vols parameter for the relevant client(s).

You could also copy a volume definition that uses the same disk image file as the bootable volume, but then set this new volume def-

inition to be non-bootable. For example, you could have the following entries in the `nvdd` configuration file:

```
...
volumes= VolXPHE, VolXP, VolXPNoBoot

VolXPHE.file=VolXPHE.vol
VolXPHE.desc="Windows XP HOME Edition"
VolXPHE.boot_device=true
...
VolXP.file=VolXP.vol
VolXP.desc="Windows XP PRO"
VolXP.boot_device=true
...
VolXPNoBoot.file=VolXP.vol
VolXPNoBoot.desc="Windows XP PRO Non Bootable"
VolXPNoBoot.boot_device=false
...
groups= group0, group1
group0.vols=VolXPHE, VolXP

...group1.vols=VolXPHE, VolXPNoBoot
```

Users of clients belonging to `group0` will have the choice to boot from `VolXPHE` or `VolXP`.

Users of clients belonging to `group1` will have no boot menu, will boot from `VolXPHE` and will see two volumes, their boot volume (`VolXPHE`, usually mounted on `C:`) and another volume, `VolXPNoBoot`, that may be mounted on `D:`. Clients in `group0` and in `group1` can be used at the same time with no problems, as long as no client mounts `VolXPNoBoot` or `VolXP` in Admin mode.

Example nvdd.conf with Multi-Volume Support

The following example nvdd configuration file shows typical settings for multi-volume support.

```
# nvdd.conf generated by Neoware Image Manager Console

#Network Settings
address=0.0.0.0
port=2184
admin_addr=0.0.0.0
admin_port=29035
authorized_subnets=

#Server settings
max_idle_time=3600
sectors_map_size=2000000
default_save_name=true
disk_threads=1
recv_buf=131072
send_buf=131072

#Directories
client_volumes_dir=./
client_files_dir=./
bin_directory=./
certificate_file=./nimcert.pem
certificate_passwd=78gfd3sD

#
# USERS definitions
#
users=P640-149, e140-156, h00e0c5590bbf, admin, every-
body, h00e0c559475a, e90-157

P640-149.mac=00E0C559316B
e140-156.mac=00E0C554E700
h00e0c5590bbf.mac=00E0C5590BBF
admin.subnets=127.0.0.1/32
everybody.subnets=0.0.0.0/0
h00e0c559475a.mac=00E0C559475A
e90-157.mac=00E0C5570540
```

```
#
# VOLUME definitions
#
volumes=disk2, disk1

disk2.id=1
disk2.file=./disk2.vol
disk2.desc=disk2
disk2.cylinders=447
disk2.heads=255
disk2.sectors=63
disk2.floppy=false
disk2.boot_device=true
disk2.check_cvol=true
disk2.no_admin_cvol=true
disk2.write_mode=cvolwrite
disk2.cvol_mode=normal
disk2.sectors_map_size=0
disk2.client_volumes_dir=
disk2.cache_size=0
disk2.type=0
disk2.users=admin, everybody
disk2.unicast_users=admin, everybody
disk2.admin_users=admin
disk2.admin_mode_users=
disk2.normal_mode_users=
disk2.volatile_mode_users=

disk1.id=2
disk1.file=./disk1.vol
disk1.desc=disk1
disk1.cylinders=447
disk1.heads=255
disk1.sectors=63
disk1.floppy=false
disk1.boot_device=true
disk1.check_cvol=true
disk1.no_admin_cvol=true
disk1.write_mode=cvolwrite
disk1.cvol_mode=normal
disk1.sectors_map_size=0
disk1.client_volumes_dir=
disk1.cache_size=0
disk1.type=0
```

```
disk1.users=admin, everybody
disk1.unicast_users=admin, everybody
disk1.admin_users=admin, everybody
disk1.admin_mode_users=
disk1.normal_mode_users=
disk1.volatile_mode_users=

#
# GROUP definitions
#
groups=group0

group0.vols=disk1, disk2
group0.unicast=true
group0.max_ram_sectors=102400
group0.read_only=false
group0.users=admin, everybody
```

CHAPTER 18

NVDD Server Administration

This chapter describes the NVDDAdmin tool and NVDAdmin protocol commands for administering a remote NVDD server.

Introduction

The NVDAdmin protocol is used to communicate with a running nvdd program. This protocol is used between a Neoware Image Manager console and a remote NVDD server in order to retrieve the configuration file currently in use, to reload it after it has been modified, and also to get information about the clients currently attached to the server, etc. Client Builder can also use this protocol when it creates the image of the original hard disk.

The NVDAdmin protocol uses TCP. The server listens on port 29035 by default, but this port can be changed in the server configuration.

NVDAdmin clients are:

- Client Builder,
- Image Manager Console,
- NVDDAdmin tool, which is described in this chapter.

Secured NVDAdmin Protocol

Neoware Image Manager server and the clients that use NVDAdmin protocol can use SSL (OpenSSL) to encrypt communications. This is mainly dedicated to configurations where a console controls a remote server through WAN. The data sent between the console and the server are then encrypted.

Note that SSL encryption has been disabled in Neoware Image Manager 4.5. If you actually want to encrypt the communication between NVDD server and NVDAdmin clients, you can set up an SSH tunnel.

Note that the data sent by the image creation process (when Client Builder creates the image file on the server) are not encrypted for performance reasons and because image creation usually occurs on a LAN, which is more secure that a WAN.

The NVDDAdmin Tool

NVDDAdmin is a tool that implements a variety of NVDAdmin commands. Most of these commands can replace “manual” operations or operations previously devoted to third party tools. Example operations are: get the current configuration file for a remote server, copy CVol files to a remote server in order to merge the CVol with an existing image (image mirroring), launch the merge process on the remopte server, etc.

NVDDAdmin Command Syntax

The syntax for NVDDAdmin is:

```
nvddadmin -h:p:c:
```

`-h <hostname>[:<port>]`

The port number is not essential. If you do not specify the `-h` option, you will have to use the `connect` command to establish a connection to the your server.

`-p <port>`

The default port number is 29035.

`-c <trusted certificates path>`

The default certificates path is `/etc/ssl/certs/`.

`-f <filename>`

The default filename is `stdin`. If this option is specified, NVDDAdmin will execute each of the commands in the specified file, making it possible to automate complex sets of instructions.

Command Examples

```
Nvddadmin –h 127.0.0.1
```

This communicates with the server running on the same machine.

```
Nvddadmin –h Server64.paris.texas.Company28.com
```

This communicates with the server running on the machine that has the DNS name `Server64.paris.texas.Company28.com`.

```
Nvddadmin –h winsrv.company.com:29037
```

This communicates with the NVDD server listening to NVDAdmin connections on TCP port 29037, on the machine that has the DNS name `winsrv.company.com`.

NVDDAdmin Commands

Considerations Related to File Operations

All the file operations (list, transfer, create folders etc.) performed on the server are related to the 'root folder' defined on the server side. The NVDAdmin protocol cannot be used to access files on the server outside the subtree of which 'root folder' is the root.

Considerations Related to put & get Commands

The `put` and `get` commands are used to transfer a file to the server (`put` commands) or from the server to the host running NVDDAdmin (`get` commands). These commands require a 'filename' parameter. This is the name of the file to be transferred (relative to the root folder of the `nvdd` server or to the current folder of the host running NVDDAdmin). The commands can also accept a second, optional

parameter: ‘name’. This is the name of the file after it has been transferred. If this second parameter is not specified, the file keeps its original name after the transfer.

The `put` and `get` commands exist in several flavors: secured (prefix s) or non secured, with resume (prefix r). "With resume" means that the command will append the rest of the file to be transferred to the data already transferred (if any).

To perform “resume” `put` and `get` commands, the host that receives the file checks the presence of a file with the same name as the file to be transferred (the name it will have after the transfer). If such a file exists, the receiving host sends the size of the file already present to the transmitting host. The transmitting host then performs an `fseek` on the file to be transferred and reads the data in the file starting at the offset that corresponds to the size of the file already present on the receiving host. The data are sent to the receiving host and appended to the data already existing in the file on the receiving host.

Conventions

The command descriptions in this section use the following conventions:

[P] indicates that the command requires authentication using a password.

[X] indicates that the command requires an exclusive Admin connection. This also implies a password.

All commands are case sensitive and must be in lowercase.

Command Descriptions

`ping`

Ping the NVDD server.

`auth <password>`

Authentification with password. The password is the one set by the NvddPasswd tool. It will be displayed in clear text on the screen when using this `auth` command.

`nopwd`

Switch to AUTH mode when the password on the server side has not been set.

`exit`

Exit this utility.

`help`

Display basic help text.

`admin`

[P] Use single admin mode (aka exclusive admin mode, exclusive admin connection).

This mode is used to make sure that the NVDAdmin connection to the remote server is the only connection of this kind that exists. The connection is then an NVDAdmin Exclusive connection. Further exclusive NVDAdmin connection requests (either sent by NVDAdmin, by the Console or by Client Builder) will fail.

`connect <host> [<:port>]`

Connect to the specified remote host. If a connection is already established to another host, it is closed, and a new connection is established.

`put <filename> [<name>]`

[P] Copies `filename` to server without resume mode on non-secured socket.

`rput <filename> [<name>]`

[P] Copies `filename` to server with resume mode on non-secured socket.

`get <filename> [<name>]`

[P] Gets `filename` from server without resume mode on non-secured socket.

`rget <filename> [<name>]`

[P] Gets `filename` from server with resume mode on non-secured socket.

`sput <filename> [<name>]`

[P] Copies `filename` to server without resume mode on secured socket.

`srput <filename> [<name>]`

[P] Copies `filename` to server with resume mode on secured socket.

`sget <filename> [<name>]`

[P] Gets `filename` from server without resume mode on secured socket.

`srget <filename> [<name>]`

[P] Gets `filename` from server with resume mode on secured socket.

`rput <filename> <name>`

[P] Copies `filename` to server with name `name` with resume mode.

`reload`

[X] Reload `nvdd` server. This command actually performs the commands `load_conf_current.get_conf_filename`. This will load the configuration file named as current, followed by the name that has been retrieved by the `get_conf_filename` command.

In other words, if you want to make a change in the currently running nvdd configuration, you must get the current conf file name, retrieve this file (using a `get` command), modify it, push it on the

remote server as `current.<filename>` (using a `put` command), and send the reload command to the server.

`load_conf <filename>`

[X] Reload server with the specified configuration file.

Caution: *When using this command, you must make sure that existing clients that may be running and have mounted virtual volumes defined in a conf file will not be disrupted. In particular, in case the volume(s) they mounted do not exist anymore or are not shared with the same ID or volume name.*

`get_conf_filename`

[P] Prints the name of the current configuration file used by nvdd server.

`check_conf <filename>`

[P] Check validity of the specified nvdd configuration file.

`stop`

[X] Stops nvdd server.

`list [<subdirectory>]`

[P] Lists (prints) the contents of the current directory. If a subdirectory is specified, this command will list the contents of the subdirectory.

`mkdir <directory>`

[P] Creates a new directory on the server side (forward slash and backslash can be used).

`rmdir <directory>`

[P] Removes the specified empty directory on the server side.

`rm <filename>`

[P] Removes the specified regular file on the server side.

`get_users`

[P] Prints a list of IP addresses and port numbers of clients that are currently connected to nvdd server.

`get_volumes`

[P] Prints a list of volumes on nvdd.

`info_user <IP_address>:<port>`

[P] Prints information about a user (a client). (One from a list exactly as reported by the `get_users` command. This means that the port must also be specified).

`info_volume <volumeID>`

[P] Gets information about the specified volume. (One from the list obtained using the `get_volumes` command).

`rm_user <IP_address>:<port>`

[P] Removes the specified client (deletes client connection) from nvdd. (Client identification obtained using the `get_users` command).

`md5 <filename>`

[P] Computes md5sum of the specified remote file. The `Md5sum.exe` file (or `Md5sum` executable for Linux/FreeBSD) must be present in `bin_directory` on the server. `bin_directory` is specified in the `nvdd` configuration file. Another `md5sum` executable and optional parameters can be specified through the use of the appropriate settings in the conf file.

`unzip <filename>`

[P] unzip remote file. The `gunzip.exe` file (or `gunzip` executable for Linux/FreeBSD) must be present in `bin_directory` on the server. `bin_directory` is specified in the `nvdd` configuration file.

Another "decompressor" executable and optional parameters can be specified through the use of the appropriate settings in the conf file. Of course, the file to be decompressed must have been compressed previously using a file compression utility that is compatible with the decompression utility being used.

`cvolmerge <VolName> <CVolName> <DestImageName>`

[P] Patch volume name (original image file) with CVolFile specified by `CVolName` to create destination name. `CVolName` is the name of the CVol header file. The CVol header file and CVol data file must have been copied previously on the remote server, e.g. using `put` commands.

CHAPTER 19

The mPXELdr Configuration File

This chapter describes the mPXELdr configuration file and the settings that can be specified in it.

Introduction

mPXELdr can use a configuration file to set the list of NVD servers that it will try to communicate with, in addition to DHCP Option 132. This configuration file also allows the setting of several boot-time options which are described later in this chapter.

mPXELdr will query the DHCP server that downloaded it for up to eight configuration files, in a fixed predefined order, until it finds its `.ini` file. For example, assume mPXELdr is running on a machine with a MAC address (Ethernet hardware address) of `m1:m2:m3:m4:m5:m6`, and a DHCP-assigned IP address of `ip1.ip2.ip3.ip4`. mPXELdr will search for configuration files as follows:

1 `m1_m2_m3_m4_m5_m6.ini`

Search for an `.ini` file specific to the MAC address of the station.

2 `ip1_ip2_ip3_ip4.ini`

Search for an `.ini` file specific to the DHCP-assigned IP address of the station.

3 `ip1_ip2_ip3.ini`

Search for an `.ini` file common to all IP addresses starting with `ip1.ip2.ip3`.

4 `ip1_ip2.ini`

Search for an `.ini` file common to all IP addresses starting with `ip1.ip2`.

5 `ip1.ini`

Search for an `.ini` file common to all IP addresses starting with `ip1`.

6 `m1_m2_m3.ini`

Search for an `.ini` file common to all the machines with this 3-byte MAC address prefix, i.e. belonging to the same "Ethernet MAC address block". A block always corresponds to a single manufacturer, but a manufacturer might have one or several blocks and models. In a number of cases, though, the MAC address prefix may be used to identify machines with similar LAN hardware configuration.

7 `<mPXELdr boot file name with extension>.ini`

Search for an `.ini` file with exactly the same name as the Network Boot Program that was used to boot this station. For instance, if mPXELdr was renamed to `MyPXELdr.bin`, and `MyPXELdr.bin` was used to boot this station, the loader will search for `MyPXELdr.bin.ini`.

8 `mPXELdr.ini`

Search for this (hard coded) exact name, with this exact capitalization.

If at this point, no `.ini` file has been found, mPXELdr will give an error message and merely use its default options and the server list provided in Option 132 of the DHCP (if any).

This search mechanism can be used to organize a multi-level hierarchy of configuration files, from the most specific (a specific piece of hardware) to the most general (all stations, for a common default) configuration.

In order to be processed by mPXELdr, all the configuration files must be installed in the same directory as mPXELdr itself.

Contents & Syntax

- A whitespace is either a space or a TAB character. Multiple whitespaces are considered just the same as a single whitespace.
- Comments are allowed in `.ini` files. A comment starts with a leading '#', and ends with the end of the line.
- Blank lines are allowed in `.ini` files.
- Whitespaces may appear before the # sign.
- A keyword is a character string that contains no spaces. Example of valid keywords could be 'Foo', 'Bar', 'NVDServers', …
- Keywords are case insensitive.
- Keywords start at the beginning of a line, but can be preceded by whitespaces.
- Keywords are always followed by an '=' sign.
- The '=' sign can be preceded or followed by whitespaces.
- The value associated with a keyword starts with the first non-whitespace character following the '=' sign.
- A standard value terminator is a '#', a ';' a ' ' (space) or a carriage return and/or line feed (end of line control characters).

- The value ends either with a standard value terminator or with a keyword-specific terminator. Because the end of line control characters are standard value terminators, values usually do not extend across lines unless otherwise specified (keyword-specific syntax).
- Unless specified otherwise, a keyword followed by an invalid value for that keyword will cause the keyword to be ignored, and the default value (if any) for that keyword to be applied.
- Unless specified otherwise, when the value associated with a keyword is a letter, only the first letter of the value is scanned and checked for validity. It is yet perfectly valid to provide additional text after that initial value, for instance to make the `.ini` file more self-explanatory. For example,

  ```
  BootMode = SemiAutomatic
  ```

  is usually considered clearer than

  ```
  BootMode = S
  ```

  and

  ```
  PreBootPause = Y
  PreBootPause = Yeah
  PreBootPause = Yo
  ```

  are strictly equivalent for mPXELdr.
- All other syntactic rules regarding a value are defined by the keyword it belongs to.

Example mPXELdr .ini File

```
# Comments are allowed in the .ini file.

# Blank lines are allowed too.

    # A ‘whitespace’ is either a space or a TAB character.
    # Whitespaces may appear before the # sign.
    # Whitespaces may appear before keywords (such as NVDServers) too.
    # Comments extend to the end of line.

# Examples of keyword use and syntax:
# Vanilla example:
# NVDServers = 192.168.0.209;

# Whitespaces can be inserted around the NVDServers
# keyword and the '=' sign.
# Keywords (like NVDServers here) are case insensitive.
# The value associated with a keyword starts with the
# first non whitespace character following the ‘=’ sign.
# The syntax of a value strictly depends on its keyword.
# What marks the end of the value is keyword dependant,
# but unless otherwise specified, values do not extend
# across lines.

#  NVDSeRveRs    =  192.168.0.209!
#  NVDServers=192.168.0.209,192.168.0.161:2300,111.111.111.111:111;

NVDServers = 192.168.0.9!    # NVD Server addition. Might have several
                            # such statements (cumulative)

NVDServers = 192.168.0.9:256,192.168.0.209:2184,192.168.0.209:10000! ;

BootMode = i      # I: Interactive, A: Auto, S: Semi-auto (default)

VolSelectionTO = 5   # Time in sec to wait for user input (max 60 s,
                     # 0 = Infinite)

PreBootPause = Yo   # <Hit any key> before boot transfer.
```

Keywords

The Include Keyword

Syntax: `Include = <Filepath>`

Examples:

```
1  Include = MyIncludeFile.ininc
2  Include = /MyIncludeFile.ininc
3  Include = SomeRelativePath/MyIncludeFile.ininc
4  Include = /SomeAbsolutePath/MyIncludeFile.ininc
```

Default value: None

The `<Filepath>` is either absolute (expressed starting relative to the TFTP root directory) or relative (to the directory where the mPXELdr boot program resides).

A leading '/' or '\' in the `<Filepath>` indicates an absolute path which will be passed "as is" to the TFTP server, while anything else indicates a relative path which will be prepended to whatever is set in the data part of the `Include` parameter.

Therefore, using examples 1 to 4 above and assuming `mPXELdr.bin` is located in subdirectory `LdrPath` of the TFTP root directory (i.e. the TFTP path of mPXELdr is `LdrPath\mPXELdr.bin`:

1 will resolve to: `LdrPath/MyIncludeFile.ininc`

2 will resolve to: `/MyIncludeFile.ininc`

3 will resolve to: `LdrPath/SomeRelativePath/MyIncludeFile.ininc`

4 will resolve to: `/SomeAbsolutePath/MyIncludeFile.ininc`

As the TFTP OS can be hosted in either a Windows, Linux or UNIX server, mPXELdr will get the default `.ini` file path from the mPXELdr file path (that comes from the DHCP information), and use the path separators ('/' or '\') that it finds there. mPXELdr will also use the path separators that it finds in the `.ini` file, whatever they are, and never alters them either. In other words, mPXELdr never inserts or removes any path separators. It merely uses those that it collects

from the PXE TFTP file path and the `.ini` file. This is important because mPXELdr has no idea whether the TFPT server is talking to a Windows, Linux or UNIX server. Even if the TFTP specification allowed such information to be known, the PXE specification is not designed to relay such information to mPXELdr.

It is the user's responsibility to use the correct separator in the DHCP parameters and `.ini` file. However, some TFTP server implementations are also path separator indifferent. This is how it should be because the TFTP client OS might be Windows, Linux or UNIX, and the TFTP client typically doesn't know either what OS and path separator convention the TFTP server is running.

Finally, it should be noted that the above rules are applied to generate a filepath (which must be no more than the PXE specification limitation of 127 bytes), and in the end that filepath is sent to the TFTP server. The result of the operation may then depend on the behavior of the TFTP server. This should not be overlooked, especially in the following areas:

- Absolute path definitions:

  If an include path definition starts with a path separator, the TFTP server might interpret the path separator as relative to the TFTP root directory OR to the host OS directory. For security reasons, the TFTP software and/or launching script should implement the former, but this should be checked with the TFTP server administrator.

- Use of '.' and '..' in paths.

  TFTP server may or may not accept or require the use of '.' to indicate the current directory and/or '..' to indicate a previous (higher) directory in the directory tree.

When mPXELdr processes an `Include` directive, it attempts to open the file passed as a parameter. If the attempt succeeds, the contents of the `Include` file is processed exactly as if it had been found in the `.ini` file being processed, at the point the `Include` directive was found.

An `Include` file may include other files. This is one of the ways to build structured configurations. `Include` files can only be nested four levels deep.

The NVDServers Keyword

Syntax: `NVDServers = <server list>`

Examples:

```
NVDServers = 192.168.0.209,192.168.0.161:2300,111.111.111.111:111;
NVDServers = 192.168.0.209,192.168.0.161:2300,111.111.111.111:111
NVDServers = 192.168.0.209,192.168.0.161:2300,111.111.111.111:111!
```

Default value: `NVDServers = ;`

The use of this keyword can replace the need of a customized DHCP Option 132, making it easier to deploy Image Manager in existing networks where DHCP servers are already installed (and sometimes not managed by the same group/department as the desktops).

The `NVDServers` keyword is used to define the list of servers that mPXELdr will try to connect to. Each server is defined by its 'dotted decimal' IP address, optionally followed by the port that the NVD server uses. If the port is not specified, the default port (2184) is used.

A server element is defined as follows:

`<IP1.IP2.IP3.IP4>[:<port>]`

Where `IP1..IP4` represent IP bytes in decimal format (value 0..255).

The `NVDServers` value is a list of server elements, separated by ',', and terminated by either a standard value terminator (cf. supra) or by an '!'.

Example of valid server lists:

```
NVDServers = 192.168.0.209,192.168.0.161:2300,111.111.111.111:111;
NVDServers = 192.168.0.209,192.168.0.161:2300,111.111.111.111:111
NVDServers = 192.168.0.209,192.168.0.161:2300,111.111.111.111:111!
```

If the terminating character is a standard value terminator or a ';', the PXE boot loader will add the TFTP server that delivered the PXE

boot file (and its `.ini` file) to the list of potential NVD servers. This is the default option.

If the terminating character is a '!', the PXE boot loader will not add the TFTP server to the list of NVD servers.

If multiple `NVDServers` keywords are found by mPXELdr during `.ini` processing, the various `NVDServers` will be processed and added to the list, and merged to build the server list according to the following rules:

The `NVDServers` enumeration will be processed in the order they are encountered and will be merged to create the boot server list, with server elements appearing in the order they were processed (i.e. left to right, in the order in which they will be encountered). If the TFTP server was added, it will appear at the point were it was first required (e.g. at the end of the `.ini` server list if the `.ini` list didn't end with a '!'). At boot time, the servers of the merged server list will be searched until one accepts the boot connection.

No duplicate will appear in the merged list (i.e. if a server appears twice in the list(s), only the first occurrence will be added to the merged list at the place it was found first). This applies also to the TFTP Server that could end up added twice if neither the `.ini` nor the Opt132 list ended with a '!', or even more if its IP address had been explicitely added to one or several `NVDServers` list.

Note: *Two servers are not considered identical if they have the same IP address, but use a different port. Thus, it is possible to include the same IP address multiple times, as long as each occurrence uses a different port.*

If the server lists are defined (or not defined) in such a way that the merged list is empty, mPXELdr will add the TFTP server to the merged list anyway and attempt to connect to an NVD server on the TFTP server at the default NVD UDP port. This makes possible the use of Neoware Image Manager server running on the same server as the TFTP server without the use of an `.ini` file or DHCP Opt132.

The use of multiple `NVDServers` lists is specifically useful when making full use of the hierarchy of `.ini` files together with the

Include directive documented in this chapter. This capability allows the administrator to create a few number of NVDServers sublists as independent files, and assemble them in different configuration files through the use of Includes in the various .ini files. This way, the whole hierarchy of server lists can be modified for large number of stations or groups of stations by simply changing a few Include files.

Yet another NVD server list can be configured in the DHCP server, as DHCP Option 132 (Opt132). The syntax of the Opt132 server list is the same as the aforementioned value for NVDServers. The Opt132 value must NOT include the NVDServers keyword nor the '=' character (Option 132 itself is the functional equivalent of the NVDServers = keyword).

If both NVDServers list(s) – in .ini files - and an Opt132 list – in the DHCP server - are defined, they will be processed in that order, and both lists will be merged using the aforementioned rules.

The BootMode Keyword

Syntax: `BootMode = <A || S || I >`

Examples:
```
BootMode = Automatic
BootMode = Semi-automatic
BootMode = Interactive
BootMode = A
```

Note: *mPXELdr only scans the first non-whitespace character that follows the '=' sign. Thus* `Atomitoc`*, even though meaningless, will be accepted and processed just the same as* `Automatic`.

Default value: `BootMode = S`

The BootMode keyword defines the behavior of the mPXELdr at boot time. It can take one of three values:

A for Automatic, S for Semi-automatic, or I for Interactive.

Automatic Mode

mPXELdr will boot off the first server it finds that:

- Answers its connection request
- Has a bootable volume this station can see and reach. The first bootable volume on the server that the station can see will be used for booting. The order of volumes on the server are defined by the server configuration.

Servers are searched in the order defined by the `NVDServers` keyword(s) (as well as Option 132), in the order specified. If the list is exhausted without a successful connection, the search will be restarted from the first server in the list, then the second, etc.

Semi-Automatic Mode

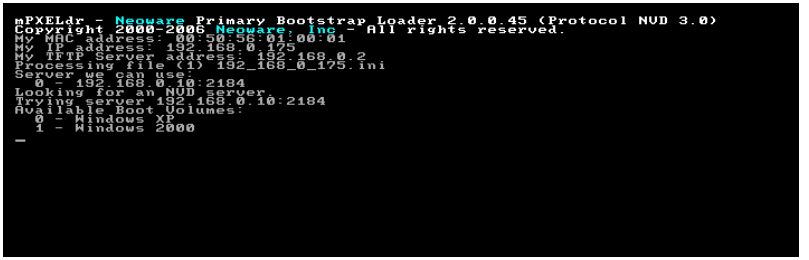
(This is the default mode if the `BootMode` parameter is not specified.)

Semi-Automatic mode is the same as Automatic mode with one exception. If the station mPXELdr is loading detects there are several volumes available for boot on the selected server, mPXELdr will switch to the Boot Volume Selection screen to allow the user to select the volume to boot from.

Boot volume selection
Use the Up and Down keys to move the highlight to your choice.
Press ENTER to choose.
Windows XP
Windows 2000
<F1> Switch to log screen - <F2> Back to this screen.

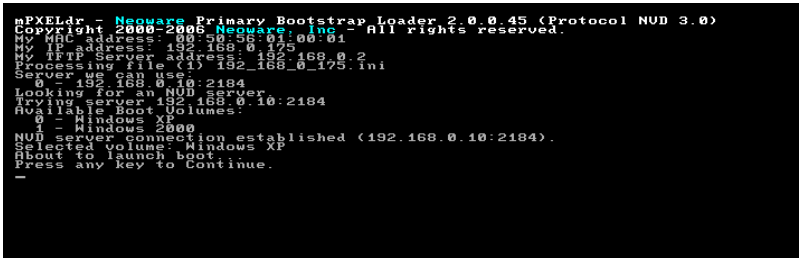
The selection is achieved using the **Up** and **Down** arrow keys then pressing the **Enter** key.

Pressing the **F1** key from this screen will change the display to the log screen which shows messages printed by mPXELdr as it runs.


mPXELdr - Neoware Primary Bootstrap Loader 2.0.0.45 (Protocol NVD 3.0)
Copyright 2000-2006 Neoware, Inc. - All rights reserved.
My MAC address: 00:50:56:01:00:01
My IP address: 192.168.0.175
My TFTP Server address: 192.168.0.2
Processing file (1) 192_168_0_175.ini
Server we can use:
0 - 192.168.0.10:2184
Looking for an NVD server.
Trying server 192.168.0.10:2184
Available Boot Volumes:
0 - Windows XP
1 - Windows 2000

Pressing the **F2** key will return you to the Boot Volume Selection screen.

The following illustration shows a typical log screen display immediately before a volume is booted. Note that this can normally only be seen if the `PreBootPause` keyword is specified and set to `Y`.

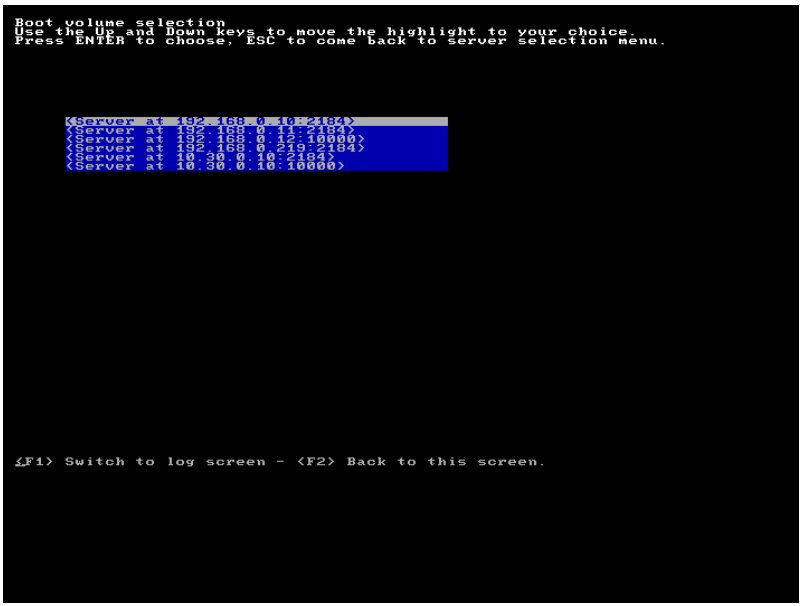

mPXELdr - Neoware Primary Bootstrap Loader 2.0.0.45 (Protocol NVD 3.0)
Copyright 2000-2006 Neoware, Inc. - All rights reserved.
My MAC address: 00:50:56:01:00:01
My IP address: 192.168.0.175
My TFTP Server address: 192.168.0.2
Processing file (1) 192_168_0_175.ini
Server we can use:
0 - 192.168.0.10:2184
Looking for an NVD server.
Trying server 192.168.0.10:2184
Available Boot Volumes:
0 - Windows XP
1 - Windows 2000
NVD server connection established (192.168.0.10:2184).
Selected volume: Windows XP
About to launch boot...
Press any key to continue.

It is possible to specify a time-out value for the interactive volume selection phase, using the `VolSelectionTO` keyword (described later in this chapter). If the time-out expires without any human action on the keyboard, the first (selected) volume on the menu will be used – basically what Automatic mode would have done.

Interactive Mode

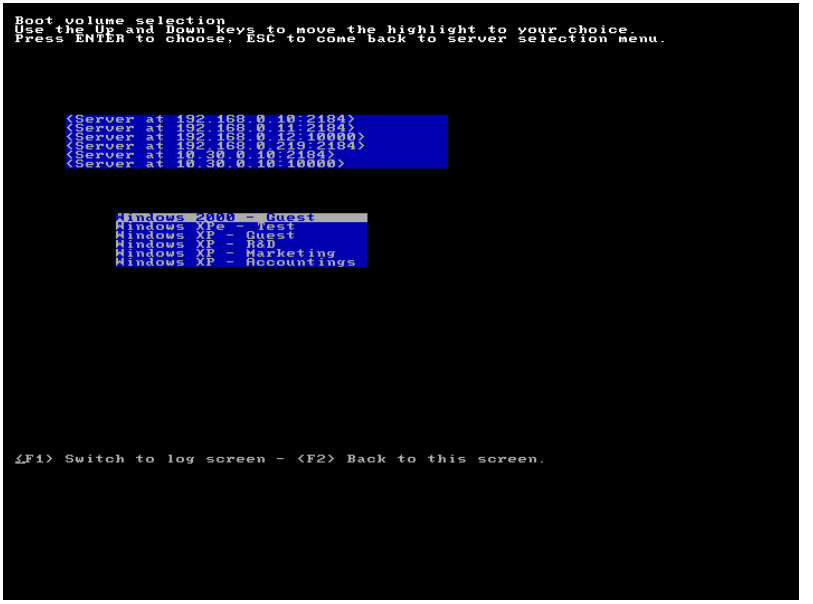
In this mode, the whole process of server and volume selection is done by the user through interactive menus.

mPXELdr first displays a Boot Volume Selection screen containing the server list build using the `NVDServers` keywords and the Option132 servers, with one entry per server found.



Server selection is achieved using the **Up** and **Down** arrow keys then pressing the **Enter** key. Note that even if there is only one server available for selection, the user still has to press **Enter** to continue.

Once a server has been selected, mPXELdr will attempt to connect to that server and display its volume list.

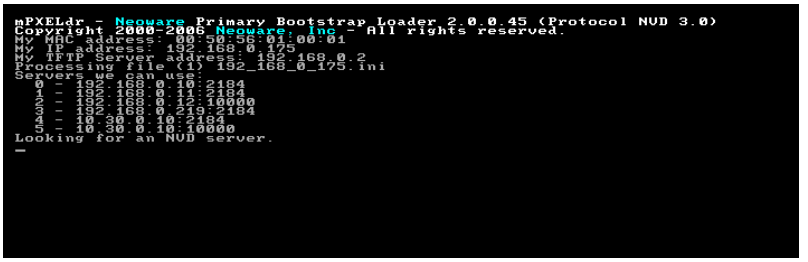


Volume selection is achieved using the **Up** and **Down** arrow keys then pressing the **Enter** key. Note that even if there is only one volume available for selection, the user still has to press **Enter** to continue. Once the user has selected and validated a volume, mPXELdr will attempt to boot that volume.

You can return to the server selection screen by pressing the **Escape** key.

Note: *The* `VolSelectionTO` *parameters described later in this chapter have NO EFFECT in interactive mode. This is by design. Interactive mode is definitely interactive, and assumes human interaction is required.*

Pressing the **F1** key from the Boot Volume Selection screen will change the display to the log screen which shows messages printed by mPXELdr as it runs.


mPXELdr - Novell Primary Bootstrap Loader 2.0.0.45 (Protocol NVD 3.0)
Copyright 2000-2006 Novell, Inc. - All rights reserved.
My MAC address: 00:50:56:01:00:01
My IP address: 192.168.0.175
My TFTP Server address: 192.168.0.2
Processing file (1) 192_168_0_175.ini
Servers we can use:
0 - 192.168.0.10:2184
1 - 192.168.0.11:2184
2 - 192.168.0.12:10000
3 - 192.168.0.219:2184
4 - 10.30.0.10:2184
5 - 10.30.0.10:10000
Looking for an NVD server.

Pressing the **F2** key will return you to the Boot Volume Selection screen.

The following illustration shows a typical log screen display immediately before a volume is booted. Note that this can normally only be seen if the `PreBootPause` keyword is specified and set to `Y`.

mPXELdr - Novell Primary Bootstrap Loader 2.0.0.45 (Protocol NVD 3.0)
Copyright 2000-2006 Novell, Inc. - All rights reserved.
My MAC address: 00:50:56:01:00:01
My IP address: 192.168.0.175
My TFTP Server address: 192.168.0.2
Processing file (1) 192_168_0_175.ini
Servers we can use:
0 - 192.168.0.10:2184
1 - 192.168.0.11:2184
2 - 192.168.0.12:10000
3 - 192.168.0.219:2184
4 - 10.30.0.10:2184
5 - 10.30.0.10:10000
Looking for an NVD server.
NVD server connection established (192.168.0.219:2184).
Selected volume: Windows 2000 - Guest
About to launch boot...
Press any key to Continue.

The VolSelectionTO Keyword

Syntax: `VolSelectionTO = <0..60 >`

Examples:
```
VolSelectionTO = 30
VolSelectionTO = 0
```

Default value: `VolSelectionTO = 10`

This keyword is only meaningful when associated with the `BootMode = S` option (see above). If the `BootMode` is set to any other value, the `VolSelectionTO` is ignored.

`VolSelectionTO` defines the number of seconds that the mPXELdr will wait to allow the user to make a selection from the list of vol-

umes available on the server. If the user does not touch the keyboard during this time period, mPXELdr will automatically select the first volume in the list and attempt to boot.

Valid values are 1 to 60 seconds. Values larger than 60 seconds are reduced to 60 seconds. A value of 0 effectively disables the time out, and will let mPXELdr wait infinitely for user interaction.

The default value is 10 (10 seconds timeout).

The PreBootPause Keyword

Syntax: `PreBootPause = <Y>`

Examples:
```
PreBootPause = Y
PreBootPause = no
```

Default value: `PreBootPause = N`

Note: *mPXELdr only scans the first non-whitespace character that follows the '=' sign. Thus Y, y and yes will be considered identical.*

This keyword accepts two values, Y and N. "N" is the default.

If set to N, boot will immediately be attempted after a volume is selected by whatever method.

If set to Y, a "press any key to continue" message will prompt the user immediately between the execution of the boot sector from the selected image.

Pressing any key will start the boot process from the selected server / volume.

The ReQueryDHCP-Options Keyword

Syntax: `ReQueryDHCPOptions = <D || N || I>`

Examples:
```
ReQueryDHCPOptions = Discover
ReQueryDHCPOptions = None
ReQueryDHCPOptions = Inform
```

Default value: `ReQueryDHCPOptions = I`

Warning: *This option implements a work around for a few and limited number of technical issues related to very specific DHCP implementations. It should only be used when such a case has been clearly and unambiguously identified.*

Before booting from the image, mPXELoader has to re-issue a query to the DHCP server in order to ensure it gets all the DHCP options that have been set (in the DHCP configuration) for the booting station. The reason this is required is because the PXE firmware only queries a limited set of DHCP options, and a few options that Windows needs do not belong to this set.

The regular way of accomplishing this is through the use of a DHCPINFORM DHCP request, and this is what mPXELoader uses. But it appears that certain versions/revisions of some DHCP servers do not process the DHCPINFORM request in a conformant way, resulting under certain circumstances in incorrect, empty or missing DHCP values in the client.

This keyword accepts three values, D, N and I. "I" is the default.

If set to D, mPXELoader will use an alternate method, DHCPDISCOVER, to request the option parameters from the DHCP server. This use of the DHCPDISCOVER slightly streches the interpretation of the DHCP specifications, but usually works and can be tried as an alternative method to the regular DHCPINFORM method.

Note that versions of mPXELdr prior to the one shipped with Image Manager v4.6.0 (and all versions of PXEOSLDR.bin) were using DHCPDISCOVER.

If set to N, mPXELoader will not do any kind of DHCP requery and will simply pass to the booting OS the options subset that the DHCP

server returned to the station in its DHCPACK reply to the DHCP request emitted by the PXE boot prom.

If set to I, the regular DHCPINFORM method is used. This is the default.

The NICRxTxQs Keyword

Syntax: `NICRxTxQs = <n1/n2>`

Examples:
```
NICRxTxQs = 8/4
NICRxTxQs = 1/1
```

Default value: None

Warning: *This option implements a work around for a few and limited number of technical issues related to very specific PXE implementations. It should only be used when such a case has been clearly and unambiguously identified.*

Both `n1` and `n2` must be in the range 1..127.

The PXE firmware internally use buffer queues for packet transmission and reception. Those queues allow the unattended transmission and reception of data packets at times when the CPU is busy doing some other work. Upon initialization, mPXELoader queries the PXE firmware for the size of the transmit and receive queue for the PXE NIC. During the boot sequence, PXE never requests from the server more packets than the Tx queue can handle. Conversely, it never attempts to send in a row more packets than the transmit queue can handle.

Unfortunately, some PXE implementations return invalid values to mPXELoader. When those values are very obviously invalid, mPXELoader detects this and assumes valid and safe (and somehow slow) values. But if those values are both invalid and plausible, mPXELoader takes them for granted and uses them. This can result in mPXELoader requesting more packets from the server than the NIC can handle and buffer, and data packet drops, timeouts, retries, etc. The result is a failing (or extremely slow) first boot phase. This has been specifically reported in the case when mPXELoader was running in a Microsoft Virtual Server or Microsoft Virtual PC virtual machine, using the MS simulated PXE NIC.

The NICRxTxQs parameters overrides the values that mPXELoader got from the PXE firmware with the values supplied.

On a general basis, without specific knowledge about the NIC implementation, values above 48/1 are unsafe and should probably not be used.

CHAPTER 20

Neoware Active Cloner

This chapter describes how to use Neoware Active Cloner to clone the current system partition to another partition.

Introduction

Neoware Active Cloner is a partition duplicator that works on a file by file basis and enables differential cloning and duplication of the current system partition to another partition while Windows is running. The Active Cloner enables very easy back-up operations and allows for optimized image update processes when used with Neoware UbiBoot.

When you run Neoware Active Cloner the following steps occur by default, but you can disable any of these steps:

1. Any files or directories on the target partition that are not on the source partition are deleted.
2. Each file on the source partition is copied to the target partition, unless the file already exists on the target partition and has the same time stamp and file size.
3. Registry files are created on the target partition.
4. By default, Neoware Image Manager Client components are disabled on the target partition so that when the target partition is used to boot Windows on a PC, Windows does not try to mount any Neoware Virtual Drive. However, when cloning to a partition in a Neoware Virtual Drive, the user can choose to keep Neoware Image Manager Client components activated on

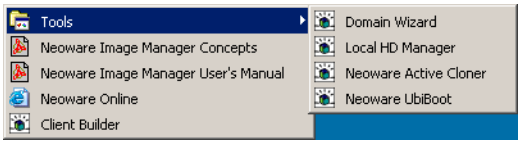
the target partition so that it stays bootable from an Image Manager server.

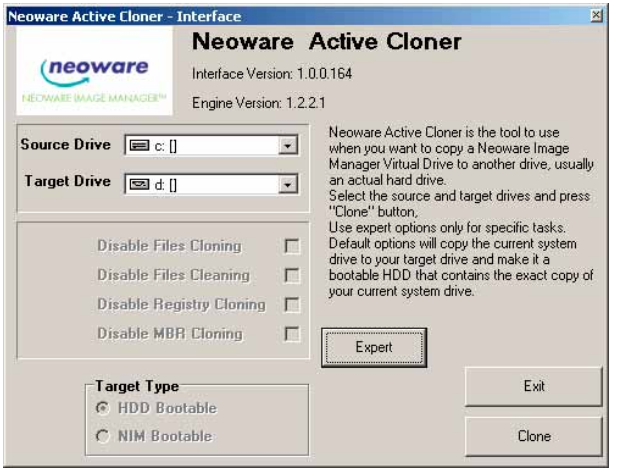
5 The Master Boot Record (MBR) of the source partition is duplicated to the target partition.

Cloning a Partition

Neoware Active Cloner can be run using command line options (described later in this chapter) or through a graphical user interface called `NimClonerGUI.exe`. The following procedure describes the basic user interface operation. Examples of the procedures used for different requirements are described in the next section.

1 To run Neoware Active Cloner from the **Start** menu, select **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Active Cloner**.




Neoware Active Cloner - Interface
Neoware Active Cloner
Interface Version: 1.0.0.164
Engine Version: 1.2.2.1
Source Drive
c: []
Target Drive
d: []
Disable Files Cloning
Disable Files Cleaning
Disable Registry Cloning
Disable MBR Cloning
Neoware Active Cloner is the tool to use when you want to copy a Neoware Image Manager Virtual Drive to another drive, usually an actual hard drive.
Select the source and target drives and press "Clone" button.
Use expert options only for specific tasks.
Default options will copy the current system drive to your target drive and make it a bootable HDD that contains the exact copy of your current system drive.
Expert
Exit
Clone
Target Type
HDD Bootable
NIM Bootable

2 The **Source Drive** is the partition to be cloned and is, by default, the partition running the operating system currently being used.

3 The **Target Drive** must be specified as a drive letter. It can be a hard disk partition attached to the Neoware Image Manager client, another Neoware Image Manager virtual hard disk, a bootable partition on a drive shared on the network, etc.

The additional options in this dialog are accessed by clicking the **Expert** button. Refer to the section "Expert Options" on page 276 for details.

4 Click the **Clone** button to start the cloning process.

The default settings will copy the current system partition to the specified target partition and make it a bootable hard disk that contains an exact copy of the current system partition.

Any errors that occur during cloning will be recorded in a log file that will be displayed in a window at the end of the process.

You can interrupt the cloning procedure by clicking the **Stop Cloning** button. A confimation dialog will be displayed. If you confirm that cloning is to be stopped, there is a high probability that the target drive will not be bootable or will not have the complete set of features that the source drive had.

Example Cloning Procedures

Cloning Directly to an Attached Hard Disk

To clone the current system drive to a hard disk attached to the computer that will be running Neoware Active Cloner so that you can boot off the attached hard disk, you must perform the following steps:

1 Make sure the attached drive has been partitioned and formatted under Windows NT (3.51, 4), Windows 2000, Windows XP or Windows 2003 OS using Windows disk management tools.

2 Make sure the partition you want to make bootable on the attached hard disk is activated and is the first partition on the hard disk.

3 If the source hard disk is the system drive that will run Neoware Active Cloner, close as many applications and services as possible. *Do not launch any applications on this computer while Neoware Active Cloner is running*.

4 Start Neoware Active Cloner.

5 Specify the **Target Drive** in the Neoware Active Cloner as the drive letter associated with the first partition on the attached hard disk.

6 Click the **Clone** button.

Cloning to a Network Shared Hard Disk

To clone the current system drive to a hard disk currently shared on the network, you must perform the following steps:

1 Make sure the shared drive has been partitioned and formatted under Windows NT (3.51, 4), Windows 2000, Windows XP or Windows 2003 OS using Windows disk management tools.

2 Make sure the partition you want to make bootable on the shared hard disk is activated and is the first partition on the hard disk.

3 Make sure the shared hard disk root directory is shared on the network.

4 Connect a network drive from your current Neoware Image Manager client to the shared hard disk. Make sure that you use connection credentials that give you full control permissions on the shared hard disk.

5 If the source hard disk is the system drive that will run Neoware Active Cloner, close as many applications and services as possible. *Do not launch any applications on this computer while Neoware Active Cloner is running.*

6 Start Neoware Active Cloner.

7 Specify the **Target Drive** in the Neoware Active Cloner as the drive letter associated with the shared hard disk.

8 Click the **Clone** button.

When the target drive is a network share, Neoware Active Cloner does not have physical access to the target hard drive and then it cannot check that the partition is activated nor can it dump the MBR of the source drive to the MBR of the target drive. Neoware Active Cloner may display messages about this, but as long as the MBR is correct and the partition has been activated, your target drive should boot correctly.

Cloning to Another Image Manager Virtual Hard Disk

To clone the current system drive to a virtual hard disk housed on the Neoware Image Manager server, and you want to be able to boot off that virtual hard disk later, you must perform the following steps:

1 Make sure the target drive was previously bootable and could be used by Windows as a boot drive.

2 Configure the NVDD server module so that it shares the target virtual drive to the client that will run Active Cloner, as a *NON-BOOTABLE* drive. This target drive will then be mounted as an extra drive (`D:`, `E:`...).

3 If the source hard disk is the system drive that will run Neoware Active Cloner, close as many applications and services as possible. *Do not launch any applications on this computer while Neoware Active Cloner is running.*

4 Start Neoware Active Cloner.

5 Specify the **Target Drive** in the Neoware Active Cloner as the drive letter associated with the target virtual hard disk.

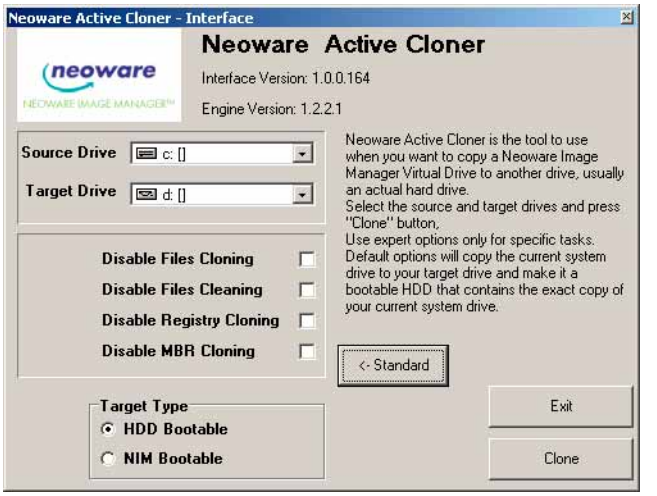
6 Click the **Expert** button to enable the additional options in the dialog box.

7 Select **NIM Bootable** as the **Target Type**.

8 Click the **Clone** button.

Expert Options

Clicking the **Expert** button will enable you to access the additional options in the dialog.


Neoware Active Cloner - Interface
Neoware Active Cloner
Interface Version: 1.0.0.164
Engine Version: 1.2.2.1
Source Drive
c: []
Target Drive
d: []
Neoware Active Cloner is the tool to use when you want to copy a Neoware Image Manager Virtual Drive to another drive, usually an actual hard drive.
Select the source and target drives and press "Clone" button,
Use expert options only for specific tasks.
Default options will copy the current system drive to your target drive and make it a bootable HDD that contains the exact copy of your current system drive.
Disable Files Cloning
Disable Files Cleaning
Disable Registry Cloning
Disable MBR Cloning
<- Standard
Target Type
HDD Bootable
NIM Bootable
Exit
Clone

Disable Options

The **Disable** options enable you to modify the cloning process so that certain steps are not included.

Selecting **Disable Files Cloning** will prevent file processing.

To prevent any files or directories on the target partition that are not on the source partition from being deleted, select **Disable Files Cleaning**. This option will have no effect if **Disable Files Cloning** is selected.

If you select **Disable Registry Cloning**, the full set of registry files will not be created on the target drive.

To prevent the duplication of the source partition Master Boot Record (MBR) to the target partition, select **Disable MBR Cloning**.

Boot Options

The **Target Type** option can be set to **HDD Bootable** (default) or **NIM** (Neoware Image Manager) **Bootable**.

Selecting **HDD Bootable** will modify the Windows settings on the target partition so that it will not include Image Manager client specific settings that makes a Neoware Virtual Drive bootable with Neoware Image Manager.

Selecting **NIM Bootable** when the source partition is already a Neoware Virtual Drive will have no effect on the Windows configuration cloned to the target partition. The cloned installation will remain Image Manager bootable.

Command Line Options

A command line engine called `NimCloner.exe` can be used to execute cloning operations from the command line instead of using the graphical user interface. This is useful for automated scripts (for example, for automatic provisioning of actual hard disk drives from virtual drives).

The command line syntax is as follows:

```
NIMCloner.exe <Destination Drive> [/Source:<Drive Letter>] [/NoFiles] [/NoCleanFiles] [/NoReg] [/NoHDDBoot] [/NoMBR] [/NoWaitOnExit]
```

The first parameter is *always* the target (destination) drive. The other parameters are optional.

The two files `NRDmpSvc` and `VVSAToolsDLL.DLL` must be in the directory from which `NimCloner.exe` is invoked.

The command line options are as follows:

`/Source:`

This specifies the source drive used as the master for cloning. It must always be followed by a drive letter. By default, the source drive is the system drive running the current instance of Windows.

`/NoFiles`

Using this option will prevent file processing.

`/NoCleanFiles`

This option will prevent any files or directories on the target partition that are not on the source partition from being deleted. It will have no effect if `/NoFiles` is specified.

`/NoReg`

This option will prevent the full set of registry files from being created on the target drive.

`/NoHDDBoot`

If you do *not* use this option `NimCloner.exe` will modify Windows settings on the target drive so that it will not include Image Manager client specific settings that make a Neoware Virtual Drive bootable with Neoware Image Manager. Note that is possible that Windows-specific settings used to boot with Neoware Image Manager would be incompatible with HDD bootability.

If you use this option and your source drive is a Neoware Virtual Drive, no change is made to the Windows configuration on the target drive, so this target drive houses a Windows installation that remains bootable by Neoware Image Manager.

`/NoMBR`

Using this option will prevent the duplication of the source partition Master Boot Record (MBR) to the target partition.

`/NoWaitOnExit`

Using this option will stop `NimCloner.exe` prompting you to press **Enter** to exit when it finishes. It will just exit silently. This is useful if `NimCloner.exe` is used in automated scripts.

Error Messages

Could Not Copy a File

If the message `Could not copy a file` is displayed, try manually copying the file from the source drive to the target drive. Some files (such as log files, temporary files) may not actually be needed for the Windows operating system on the target drive in order to boot off the target drive. If the file cannot be copied, check if the file is actually required. You may need to run disk checking/repairing tools if some files are corrupted.

Client-Specific Settings on the Target System

When you clone a Neoware Image Manager drive to a target drive, the current client-specific details are copied to the target system. In particular, the target system will use the Computer Name, IP address and Domain Credentials that were used by the Neoware Image Manager client when Active Cloner was run. This makes automatic provisioning of HDD very efficient as you do not have to change these settings after the cloning has occurred, nor do you have to run anything after the cloning process has completed. The clients can boot immediately off the cloned HDD.

CHAPTER 21

Virtualized Environments

This chapter describes how to use Neoware Image Manager with virtual machines, which can run Image Manager clients or server.

VMWare Environment

Introduction

Neoware Image Manager integrates perfectly well in VMWare environments. It can be used to stream OS and applications (actually disks) to Virtual Machines, making it very useful in VDI (Virtual Desktop Infrastructure) environments. Neoware Image Manager Server can also run as an application or service in a Virtual Machine.

Streaming Disk Images to Virtual Machines

Creating the Disk Image

In order to create a disk image for streaming to virtual machines, you will usually follow the standard procedures described in this manual. In particular, you will have to start from an existing installation of Windows XP or Windows 2000 guest, booted off a regular VMWare disk drive.

However, before you create your image, you should make sure that you have correctly installed the latest versions of VMWare tools for your client Guest OS. This means that the VMWare tools must be installed before you run Image Manager ClientBuilder in order to capture your disk image.

In particular, you should make sure that the latest VMWare Network Interface Card driver (VmxNet driver) is actually installed and working. Using this driver will actually improve performance and failing to use it may result in creating an image that will not be bootable by Image Manager Clients.

Adding VM Support to Existing Images

You can modify an existing Image Manager virtual drive so that it can be used to boot VMs. This virtual drive would usually be used to boot physical machines prior to enhancing it to support network booting VMs.

The easiest way to achieve this is to use UbiBoot Extractor to extract the required data from an existing VMWare guest running Windows, then use UbiBoot Inserter to insert the previously extracted data in your existing image. Refer to “Adding Network Boot Devices to an Image” on page 87 for information about using UbiBoot Extractor and Inserter.

Once your existing image has been enhanced to support VMware guest network card as a boot device, you will have to boot a VM off this image in order to install the rest of the drivers for the VM. You would usually do this operation in Admin mode (or in CVolWrite/Normal mode and then use CVolMerge to update the image).

In order to boot your VM off a Neoware Image Manager virtual disk, you must enable the VM to boot from the network using PXE (see below).

Note that it is sometimes not possible to boot a VM image without it having a VMWare virtual disk drive (.vmdk file) attached to it, even if that disk drive is not used. Therefore, you can attach the smallest possible disk drive to your VM and never partition or format it. Also, use a dynamic non-persistent disk.

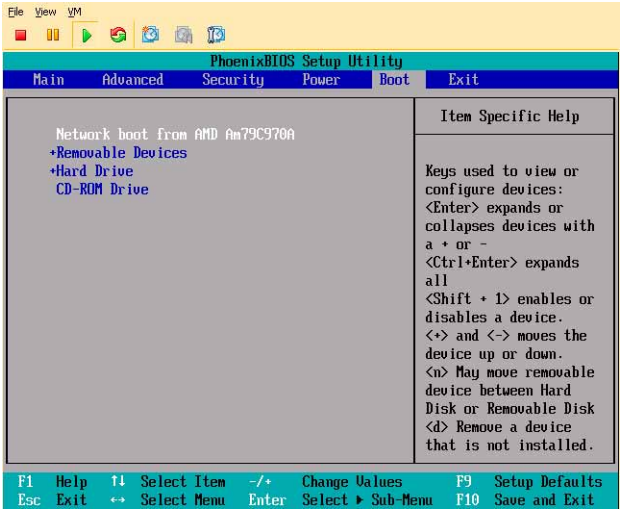
When your VM can boot off the Neoware Image Manager virtual disk, it will detect some new hardware. In order to provide the complete set of drivers, you would use VMWare tools.

When the drivers are completely installed in the image, that image can be used to boot all the machines it previously supported, including the Physical machines, and also the VMWare VMs.

Having such an image may be very convenient as you can boot it in any VMware VM and then be able to reproduce what users experimence on their machines, even if you do not have to hand any client machine compatible with the image.

Enabling PXE Boot in Your VMs

In order for your VM to be able to boot of a Neoware Image Manager virtual drive, you have to enable PXE boot. This is usually done by modifying the BIOS setting of the guest VM:


File View VM
PhoenixBIOS Setup Utility
Main Advanced Security Power Boot Exit
Network boot from AMD Am79C970A
+Removable Devices
+Hard Drive
CD-ROM Drive
Item Specific Help
Keys used to view or configure devices:
<Enter> expands or collapses devices with a + or -
<Ctrl+Enter> expands all
<Shift + 1> enables or disables a device.
<+> and <-> moves the device up or down.
<n> May move removable device between Hard Disk or Removable Disk
<d> Remove a device that is not installed.
F1 Help ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▸ Sub-Menu F10 Save and Exit

Disabling the Embedded DHCP Server

If the network interface cards in your VMs are using NAT, we recommend that you disable the VMWare embedded DHCP server, for it is not easily able to set PXE data and sometimes interferes with the actual PXE/DHCP Server.

If you are using VMWare Workstation or VMWare server, this is achieved by using the menu **Edit > Virtual Network Settings** then selecting the tab **DHCP Server** and stopping the service. You must also make sure that the DHCP Service is not running by default. For instance, under Windows, you should open the "Services" management console.

Provisioning VMs with Image Manager

Neoware Image Manager is a perfect tool for provisioning Virtual Machines that are supposed to have the same set of applications and the same usage (in VDI environments for example).

With Neoware Image Manager, as long as your VMs boot off the network, you can easily provision and manage a single virtual disk that is actually used by several servers at the same time. Actually, the operations are exactly the same as with physical machines.

Running Image Manager Server in a VM

You can run Image Manager Server in a VM. Just install your server OS (Windows or Linux) in the VM as you would do normally. Install the Neoware Image Manager the standard way. That's all!

Note: *FreeBSD has never been validated in VMWare environments.*

Using Private Networks

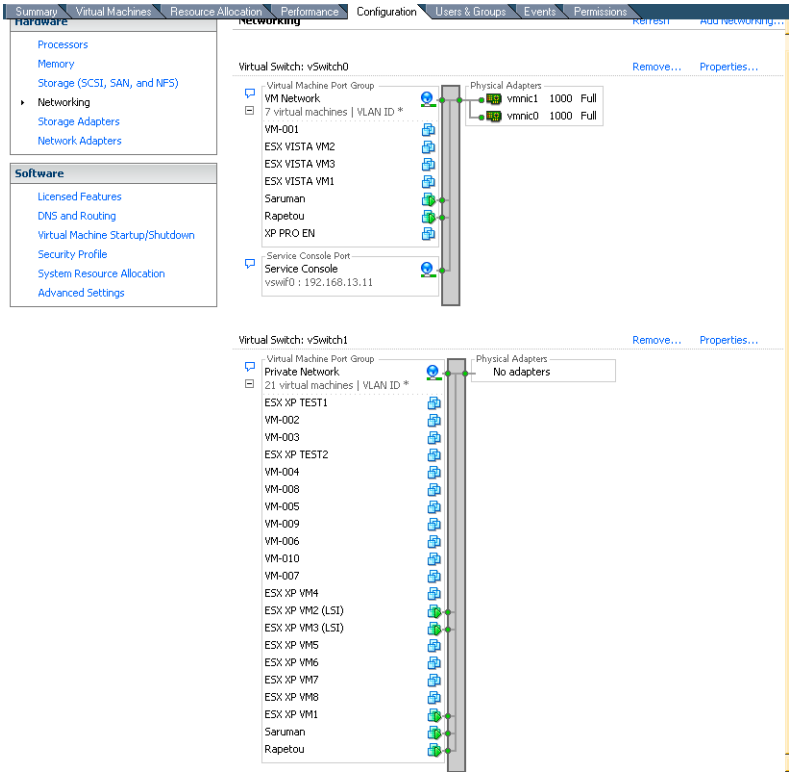
If your server and clients run in VMs on the same host, you can set a private network used only by your client VMs and your server VM. This private network would not be linked to any physical adapter in the host. All the network traffic between your Image Manager server and clients will be confined to the host. The Guest that runs Image Manager server would then also usually be a DHCP server and TFTP Server.

Using Public & Private Networks

You can configure your Image Manager server's VMs to have two virtual network interface cards, one bound to a private network, the other bound to a public network. The servers can then serve Image Manager virtual disks to VMs connected to the private network and at the same time to machines (physical or virtual) that have access to the public network.

Setting a routing service or a NAT service on the guest that runs Image Manager server would then enable it to be the gateway between the private network and public network, and machines in the private network would potentially have access to all the network resources available to the public network (internet access, network file servers etc).

Here is an example of such a private + public network configuration on a VMWare ESX server:



In the example above, the two machines named `saruman` and `rapetou` are servers that run Neoware Image Manager server module. Both have two NICs, one connected to Private Network (172.16.0.0/16), the other connected to the public network (VM Network, 192.168.1.0/24).

The server named `saruman` runs the DHCP service for Private Network. It is also configured to route IP packets between the private and public network.

When setting such a dual network configuration, administrators should be careful to configure their DHCP service so that it does not interfere with the public network if this is not desired. Usually, an administrator would create a DHCP scope or subnet that would only server the IP addresses in the private network. In the example above, the only active DHCP subnet on the server `saruman` is 172.16.0.0.

Performance & Storage Optimization

Performance in VMware environments is usually consistent with VMware usage. You will not be able to run more VMs (or less VMs) on a single host when they boot off a Neoware Image Manager virtual disk than when they boot off their own private VMware `.vmdk` disk. Yet, because you can use the very same Neoware Image Manager virtual drive to provision several VMs, you need less storage, providing that you have several VMs that use the same image.

Image Consolidation

Using a common Image Manager virtual disk makes it easier to patch your VMs, install and deploy new applications etc., in the same way it makes it easier to manage physical machines. The VMs are also stateless and providing a new VM is just a matter of creating the VM. When it is created, boot it off the network. No deployment or cloning is required.

Limitations

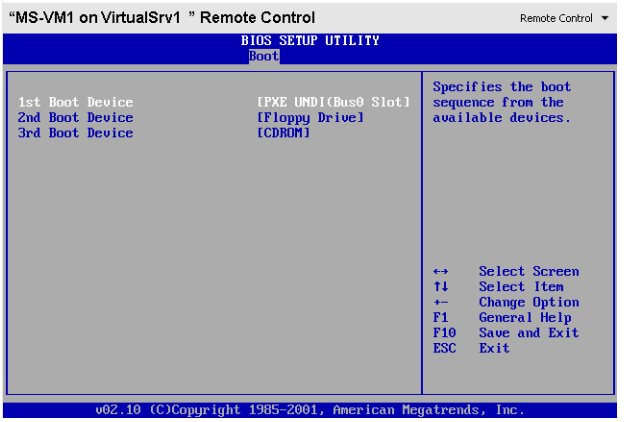
As the VMs provisioned by Image Manager are not actually using any `.vmdk` files (VMware virtual disk files), all the operations that require such files are not available when the VMs are booted off Image Manager virtual disk. This includes VMotion, snapshots, pause and resume… However, there is no obvious technical reason for these operations to require the need of a `.vmdk` file, so it is very likely that these limitations will be lifted in the next future.

Microsoft VirtualPC Virtual Server Environments

Most of what is mentioned in the previous section for VMware environments is also true in Microsoft VirtualPC/Virtual server environments. Refer to the VMware section earlier for more details about general operations with virtual machines. In this section we will focus on Microsoft VirtualPC/VirtualServer specifics.

Enabling Network Boot

To enable network boot, boot the VM, press the **Del** key to enter BIOS, go to the BOOT menu then enable network boot. For example:



Note: *The PXE code in some implementations of Microsoft VirtualPC and Virtual server VM reports an incorrect size for receive/transmit queues. This can prevent the VM from actually booting off Image Manager server. In order to correct this issue if you encounter it, please use the NICRxTxQs parameter in mPXELdr's .ini file. The correct value for use with MS VirtualPC/VirtualServer VMs is NICRxTxQs = 8/1. Please refer to "The mPXELdr Configuration File" on page 251 for more details about mPXELdr.bin initialization files.*

Other Virtualized Environments

There are other virtualized environments than VMWare and Microsoft VirtualPC/Virtual Server: Xen, Virtual Iron, VirtualBox, kvm etc. The VMs in these environments can usually be used to run Neoware Image Manager server module. However, all the “other virtualized environments” we could test implemented only partially the PXE standard and thus were not able to successfully PXE-boot off Neoware Image Manager.

Things are moving fast in the Virtualization world, so it is very likely that the “other virtualized environments” will catch up on standard compliance.

APPENDIX A

Upgrading Image Manager

This appendix describes how to upgrade from earlier versions of Neoware Image Manager.

Important

The components in a specific release of Neoware Image Manager must not be mixed with components from other releases. Components in a specific release of Neoware Image Manager are designed to work together and may not work if used with components that are not part of the same release.

Upgrading from Previous Versions of Neoware Image Manager 4

Order of Upgrading Operations

1. Backup your hard disk image.
2. Boot one client with the older version of Neoware Image Manager.
3. Configure `nvdd` so that the virtual volume (virtual HD) is mounted in Admin mode by this client.
4. Using this client, run Client Builder from the newer version of Image Manager (launched from the CLIENT folder that contains the newer components). It detects that it is actually performing an upgrade.

If there are WiFi adapters in the list of supported Network cards, check the **Expert** option and make sure that no WiFi adapter is selected.

5 Shutdown the client.

6 Stop `nvdd` server.

7 Replace the server modules (`nvdd.exe`, `mPXELdr.bin`) and the server tools (CVolMerge, CVolCompactor, NvddPasswd, NvddAdmin) on the server side. You can perform a **Server** installation after having uninstalled the previous version, or you can use **Decompress** installation to get the files you need.

8 Launch the console shipped with v4.6.

9 Open the configuration file previously used with v4.x.x.

10 Optional: If you were previously running Image Manager v4.0 or v4.1, in **Tools** > **Generic Options** > **Directories** set the path for the certificate to the certificate shipped with Image Manager 4.6 (`nimcert.pem`, in the `Server` directory. Usually, you would just need to enter `nimcert.pem` in the field).

11 Optional: If you were previously running Image Manager v4.0 or v4.1, enter a password in the **Password** field (this field is not currently used but must be filled!). Optionally change the other directories/path parameters (the default values should work correctly, so you may just leave them as the console sets them, that is ‘./’ (meaning the folder where `nvdd.exe` is located)).

12 Change the volume write mode so that it is not in Admin mode. We recommend using CVolWrite/Volatile mode at this point.

13 Backup the older `nvdd` server binary (`nvdd.exe` or `nvdd`). Copy the new v4.6 `nvdd` server binary in the folder that contains the older `nvdd` server binary. Launch the new v4.6 `nvdd` server so that it serves the virtual volume image you have just modified. (In order to do so, you would usually use the configuration file modified previously.)

14 Boot-up one client. It should boot with the new `mPXELdr.bin` and the new drivers from the updated image.

15 If new hardware is detected on the client (e.g. because of some changes in Neoware Image Manager client drivers), you may want to reboot the client in Admin mode so that the new hardware is detected once for all and does not have to be redetected every time a client boots up. Then change the Neoware Image Manager server configuration so that the virtual volume is not mounted in Admin mode any more.

Troubleshooting

Another way to upgrade is to dump the image to be upgraded onto a physical HDD (using Neoware Active Cloner) and perform the standard install process, run the new `nvdd.exe` so that it shares `smalldisk`, run Client Builder and build your image.

APPENDIX B

The TFTPD Installer

This appendix describes how to use the TFTPD Installer to configure Windows 2000/2003/XP TFTP Server for Image Manager clients.

Introduction

The TFTPD Installer is a tool for helping you to install the TFTP server (TFTPD) that is shipped with Microsoft Windows 2000/ 2003 Server, so that it can be used with Neoware Image Manager clients.

Note that the Microsoft TFTP Server is designed to be used only on the Windows 2000/2003 and XP operating systems, if you have the valid licenses. For Windows NT you can use 3Com® freeware TFTP Server that can be downloaded from the following link:

`ftp://ftp.3com.com/pub/utilbin/win32/3CTftpSvc.zip`

The freeware `TFTPD32` (`http://www.jounin.net`) can also be used as TFTP server (not running as a service) and as a simple DHCP server (also not running as a service).

To install Microsoft TFTP Server, you will require Windows 2000/ 2003 Server installation media (usually a CD-ROM).

Using the TFTPD Installer

The following procedure assumes that the Microsoft TFTPD service is not yet installed. If the service is already installed, the TFTPD Installer will behave slightly differently to what is described here. However, the messages and hints displayed by the TFTPD Installer should still enable you to use it easily.

1 Run the TFTPD Installer, either from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **MS-TFTP Server Helper**, or by navigating the file system: `<decompressed archive root directory>/Image_Manager_4.6/Server/Windows/TFTPDInstall.exe`.

Neoware Image Manager™ MS-TFTPD Installer v2.1.1.3
neoware
TFTPD Installation tool
This utility is designed to help you installing the TFTP server (TFTPD) that is shipped with MS-Windows 2000/2003 Server. You will need MS Windows 2000/2003 server installation CD-ROM (or installation files).
Path to Windows 2000/2003 Server files
D:\I386
Path to TFTP Served files root folder
C:\tftpboot
Create folder C:\tftpboot
Run TFTPD Service now
Run TFTPD Service at boot time
Apply
Close

2 In the **Path to Windows 2000/2003 Server files** field, specify the path to the directory containing Windows 2000/2003 Server installation files (usually a subdirectory called `I386`).

The TFTPD Installer will search this directory for a file named `TFTPD.EX_` or `TFTPD.EXE`.

3 In the **Path to TFTP Served files root folder** field, specify the location of the directory that will contain the files to be served by the TFTP Server. This can either be a directory that is already defined, or you can enter a new directory name and check the **Create folder** box to create it automatically when you click the **Apply** button later.

4 It is recommended that you check the **Run TFTPD Service at boot time** box so that TFTP Server will be launched automatically when the server boots.

5 If you want the TFTPD Service to be run when the TFTPD Installer is exited or when you click the **Apply** button, check the **Run TFTPD Service now** box.

6 Click the **Apply** button.

7 Click **OK** to exit the TFTPD Installer.

8 Make sure that the file `mPXELdr.bin` (or `mPXELdr.<ServerMACAddress>.bin`) is present in the directory you specified in the **Path to Windows 2000/2003 Server files** field. You may need to copy the file from the Neoware Image Manager `Server` directory.

9 If the following information message is displayed, restart the server to run TFTPD.

Managing the TFTPD Service

Once Microsoft TFTP Server is installed, you can manage the TFTPD service using the standard tools for managing services. For example, if you want to change the way TFTP Server is launched at boot time, you can right-click on **My Computer**, select **Manage** > **Services** > **TFTPD Service** to enable you to change the setting.

APPENDIX C

Configuring the DHCP Server

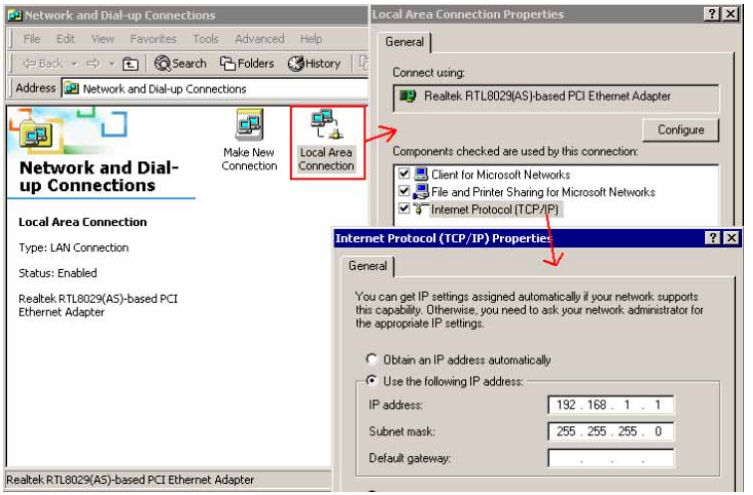
This appendix describes how to configure the Windows 2000/2003 DHCP server.

Introduction

This appendix describes how to install and configure Microsoft DHCP Server, supplied with Windows 2000/2003 Server, for use with Neoware Image Manager.

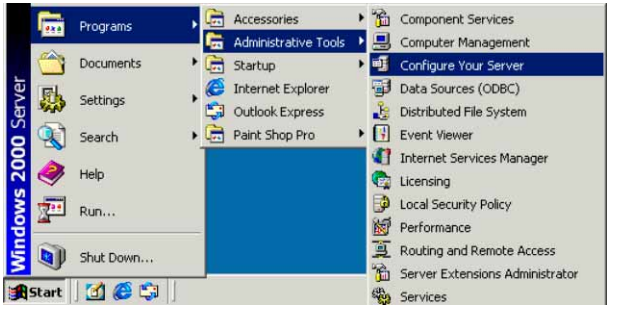
Before Installing DHCP Server

IMPORTANT: The system on which DHCP server is to be installed ***must*** use a static (i.e. manually assigned) IP address:

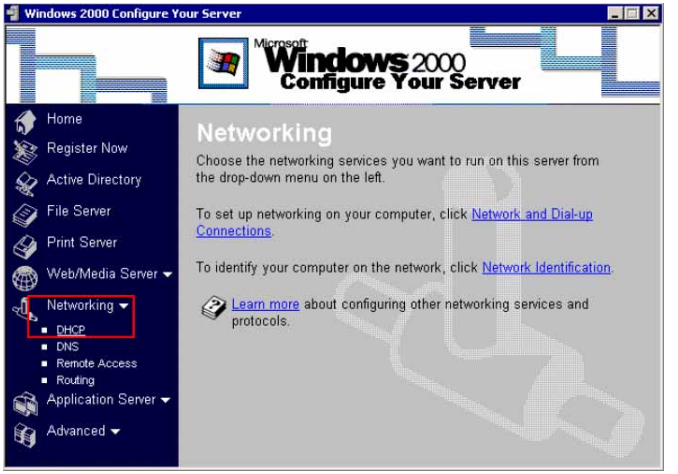

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Network and Dial-up Connections
Make New Connection
Local Area Connection
Local Area Connection
Type: LAN Connection
Status: Enabled
Realtek RTL8029(AS)-based PCI Ethernet Adapter
Realtek RTL8029(AS)-based PCI Ethernet Adapter
Local Area Connection Properties
General
Connect using:
Realtek RTL8029(AS)-based PCI Ethernet Adapter
Configure
Components checked are used by this connection:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway:

Configuring the Server

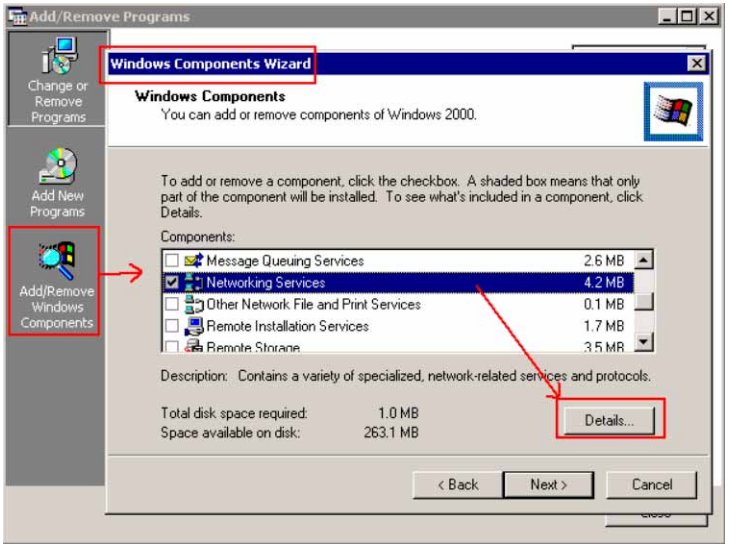
Like with all other Server related components, you can start the setup of the DHCP server by selecting **Configure Your Server** from the **Start/Programs/Administrative Tools** menu.



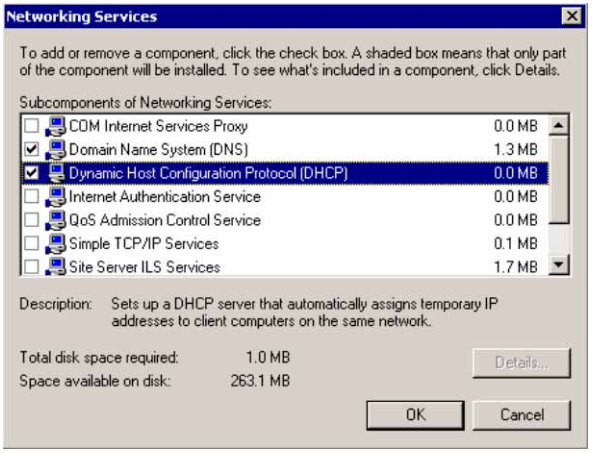
1 From the **Start** menu, select **Programs** > **Administrative Tools** > **Configure Your Server** to display the following dialog:



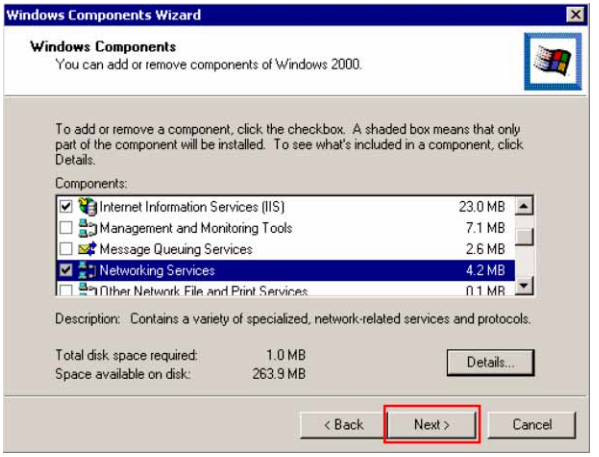
2 In the left-hand panel, click on **Networking**, select **DHCP**, and then start the **Windows Component Wizard**. (This wizard can also be started from the Control Panel by selecting **Add/Remove Programs**, then **Add/Remove Windows Components**.)


Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Windows Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Message Queuing Services 2.6 MB
Networking Services 4.2 MB
Other Network File and Print Services 0.1 MB
Remote Installation Services 1.7 MB
Remote Storage 3.5 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 1.0 MB
Space available on disk: 263.1 MB
Details...
< Back
Next >
Cancel

3 Click on the line **Networking Services** and then click the **Details...** button.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
COM Internet Services Proxy 0.0 MB
Domain Name System (DNS) 1.3 MB
Dynamic Host Configuration Protocol (DHCP) 0.0 MB
Internet Authentication Service 0.0 MB
QoS Admission Control Service 0.0 MB
Simple TCP/IP Services 0.1 MB
Site Server ILS Services 1.7 MB
Description: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network.
Total disk space required: 1.0 MB
Space available on disk: 263.1 MB
Details...
OK
Cancel

4 Locate the line **Dynamic Host Configuration Protocol (DHCP)** in the list box and check the check box next to it. Click the **OK** button to continue.


Windows Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Internet Information Services (IIS) 23.0 MB
Management and Monitoring Tools 7.1 MB
Message Queuing Services 2.6 MB
Networking Services 4.2 MB
Other Network File and Print Services 0.1 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 1.0 MB
Space available on disk: 263.9 MB
Details...
< Back
Next >
Cancel

5 Click **Next** in the **Windows Components** dialog.

A progress bar will be displayed while the system configures the network components.

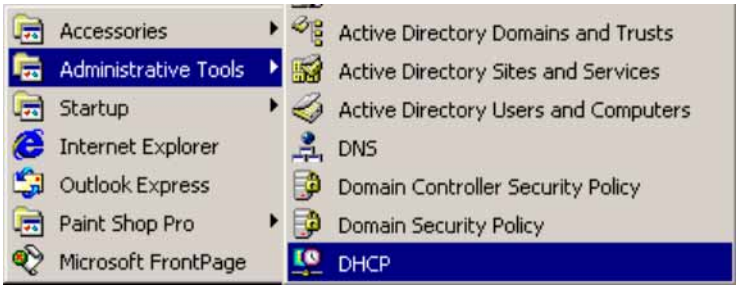
Windows Components Wizard
Configuring Components
Setup is making the configuration changes you requested.
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.
Status: Completing configuration of DHCP Protocol...
< Back
Next >

6 When the Windows Components Wizard has successfully completed, click the **Finish** button.

Configuring DHCP

The DHCP server must be configured before it can be used.

1 From the **Start** menu, display the **Administrative Tools** menu and select **DHCP**.

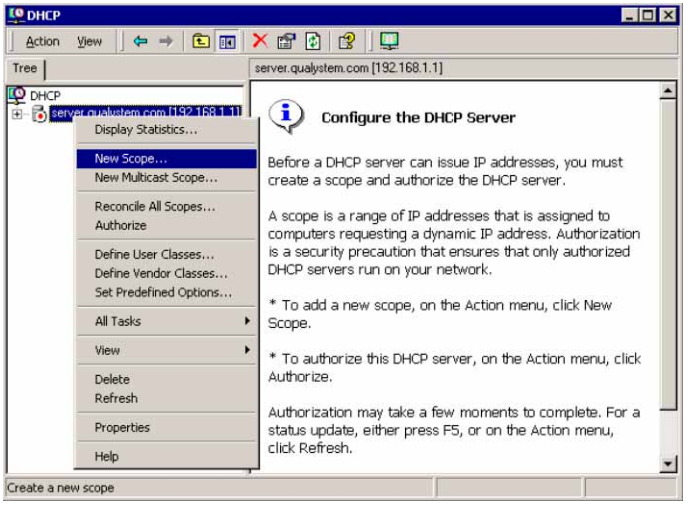


In the left pane of the **DHCP** window you will see the name and IP address of the DHCP server.

After installation, a DHCP server is *not authorized*. Do not forget this later!

2 You need to define the range of IP addresses to be assigned (i.e. distributed) by the DHCP server. A definition of a range of IP addresses (with or without additional options) is called a *scope*.

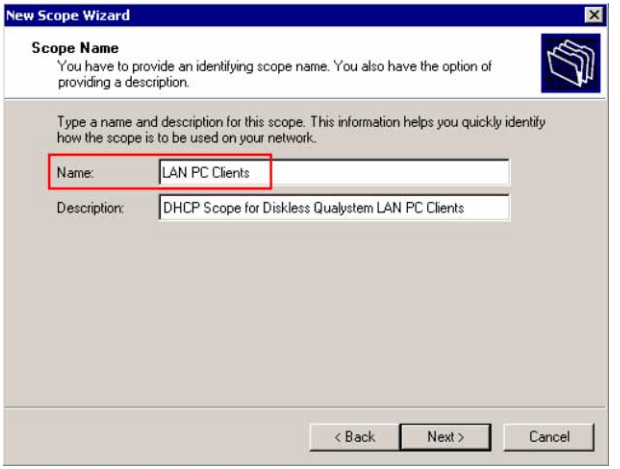
Select your DHCP server and then either with a right-click or from the **Action** menu, select to define a **New Scope**.


DHCP
Action
View
Tree
server.qualystem.com [192.168.1.1]
DHCP
Display Statistics...
New Scope...
New Multicast Scope...
Reconcile All Scopes...
Authorize
Define User Classes...
Define Vendor Classes...
Set Predefined Options...
All Tasks
View
Delete
Refresh
Properties
Help
Configure the DHCP Server
Before a DHCP server can issue IP addresses, you must create a scope and authorize the DHCP server.
A scope is a range of IP addresses that is assigned to computers requesting a dynamic IP address. Authorization is a security precaution that ensures that only authorized DHCP servers run on your network.
* To add a new scope, on the Action menu, click New Scope.
* To authorize this DHCP server, on the Action menu, click Authorize.
Authorization may take a few moments to complete. For a status update, either press F5, or on the Action menu, click Refresh.
Create a new scope

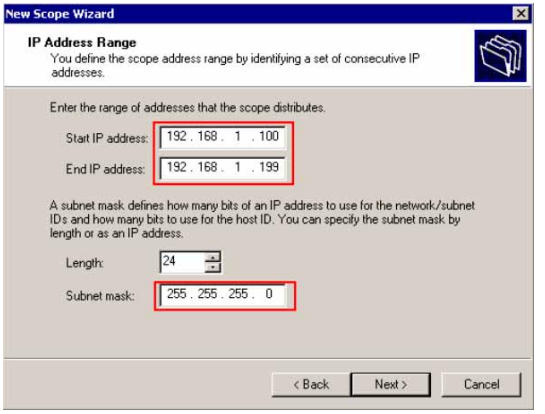
This will open the **New Scope Wizard**.

New Scope Wizard
Welcome to the New Scope Wizard
This wizard helps you set up a scope for distributing IP addresses to computers on your network.
To continue, click Next.
< Back
Next >
Cancel

3 Click **Next** to continue.


New Scope Wizard
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
LAN PC Clients
Description:
DHCP Scope for Diskless Qualystem LAN PC Clients
< Back
Next >
Cancel

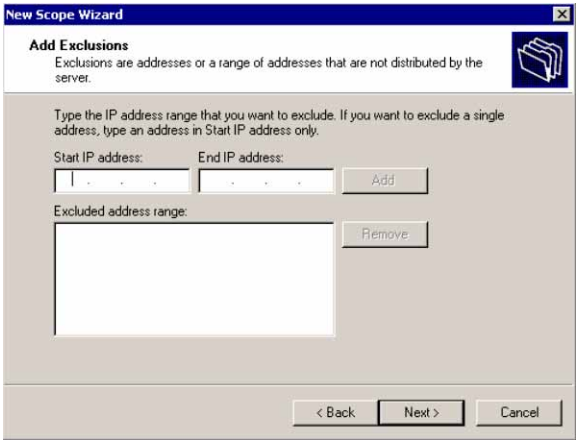
4 Enter a name and description for the scope you are about to create, then click **Next**.


New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Enter the range of addresses that the scope distributes.
Start IP address:
192 . 168 . 1 . 100
End IP address:
192 . 168 . 1 . 199
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.
Length:
24
Subnet mask:
255 . 255 . 255 . 0
< Back
Next >
Cancel

5 Specify the range of IP addresses and the subnet mask. The range must not include the IP address of the DHCP server itself, or any other device with a manually assigned IP address (e.g. network printers).

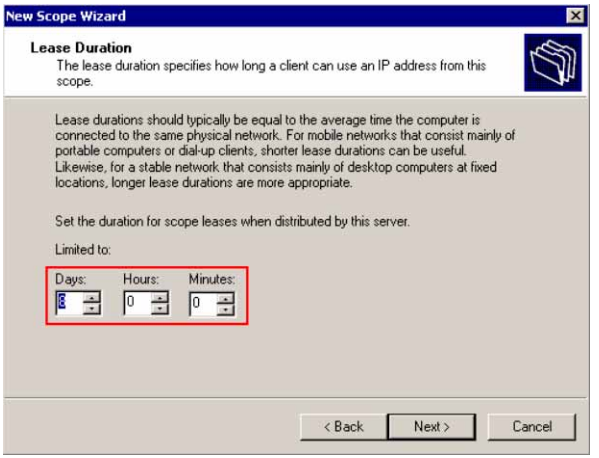
Although you could exclude them in the next step, usually a range is reserved for manually assigned addresses and then the rest (in this case 100 - 199) is given to the DHCP server for automatic distribution.

6 Click **Next** to continue.


New Scope Wizard
Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address:
End IP address:
Add
Excluded address range:
Remove
< Back
Next >
Cancel

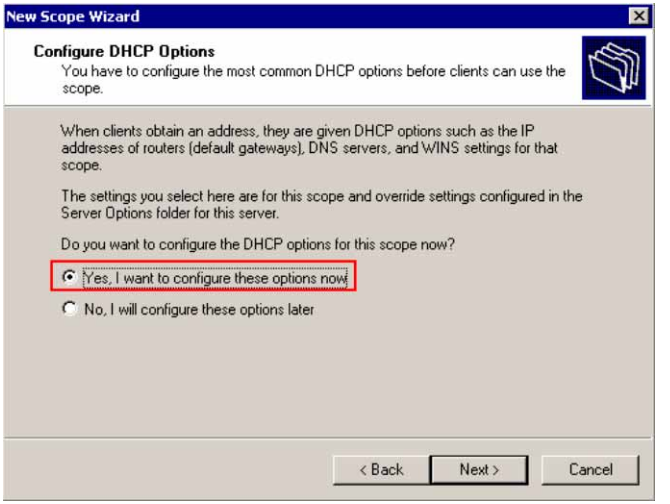
7 If you could not define separate ranges for manually-assigned and DHCP-assigned IP addresses, then you can define the addresses to be excluded and not to be used by the DHCP server in this **Add Exclusions** dialog.

Click **Next** to continue.

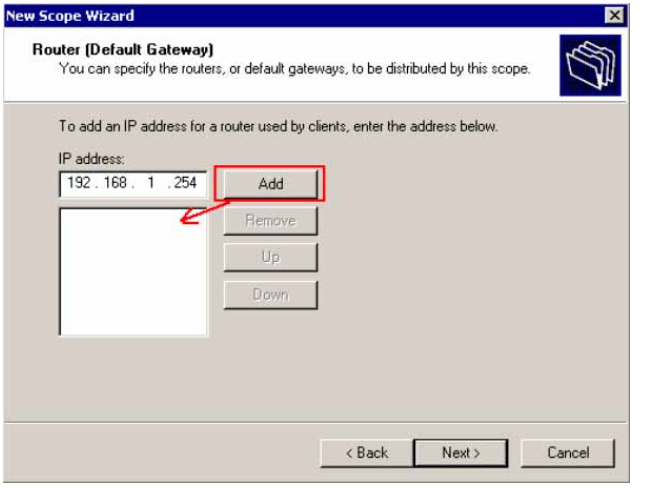

New Scope Wizard
Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.
Set the duration for scope leases when distributed by this server.
Limited to:
Days:
Hours:
Minutes:
8
0
0
< Back
Next >
Cancel

8 Typically, an IP address is assigned (i.e. leased) for a limited period of time. This avoids the situation where you run out of available addresses when visitors connect to the network and gat an IP address assigned. Without a time limit these IP addresses could not be re-used. Usually 8 days is a good choice and will ensure that workstations on the network will continue to use the same IP addresses assigned to them every day, since their systems will in time extend the lease.

9 Click **Next** to continue.


New Scope Wizard
Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.
Do you want to configure the DHCP options for this scope now?
Yes, I want to configure these options now
No, I will configure these options later
< Back
Next >
Cancel

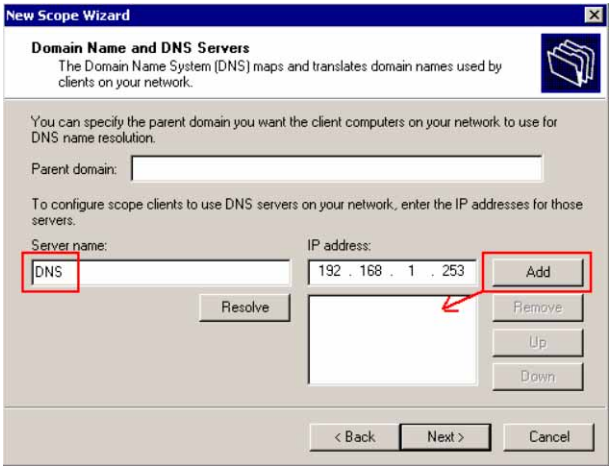
10 Additional DHCP options must be set when serving IP addresses to Neoware Image Manager clients in order for the system to work correctly. Select the option **Yes, I want to configure these options now**, then click **Next**.


New Scope Wizard
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.
To add an IP address for a router used by clients, enter the address below.
IP address:
192 . 168 . 1 . 254
Add
Remove
Up
Down
< Back
Next >
Cancel

11 Is your Neoware Image Manager clients network part of a Wide Area Network? Do you want Neoware Image Manager clients to access the internet? If the answer is yes, you will need to configure the client computers with the IP address of the Gateway (or Router) to be able to communicate with systems on the WAN.

Enter the IP address then click **Add** to enter the address to the list of Gateways.

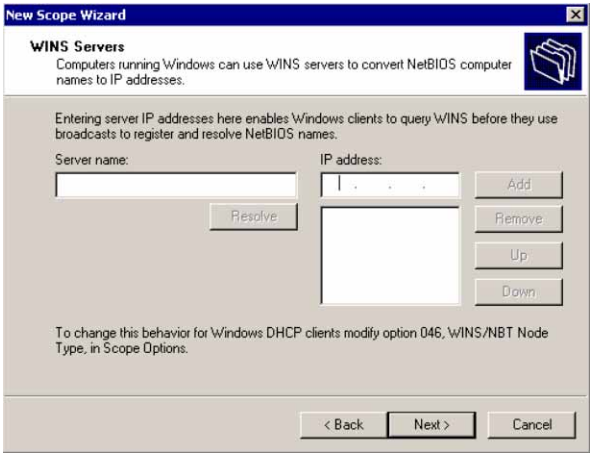
12 Click **Next** to continue.


New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
DNS
192 . 168 . 1 . 253
Add
Resolve
Remove
Up
Down
< Back
Next >
Cancel

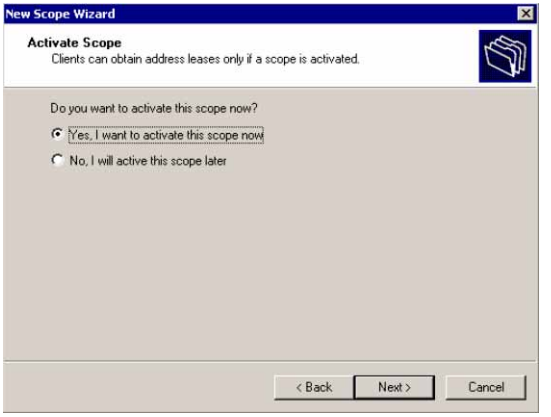
13 Are you using a WAN and need to help your clients to locate the IP addresses of servers (e.g. WebServers) on the WAN? Or do you intend to have clients connected to the Windows 2000 server via the new Active Directory methd? If the answer is yes you must configure the clients to use a DNS server.

Enter the name of the DNS server and its IP address then click **Add** to add the entry to the list.

14 Click **Next** to continue.


New Scope Wizard
WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.
Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.
Server name:
IP address:
Add
Resolve
Remove
Up
Down
To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.
< Back
Next >
Cancel

15 The **WINS Servers** dialog enables you to enter WINS server IP addresses that computers can use to convert NetBIOS computer names to IP addresses. Click **Next** to continue.

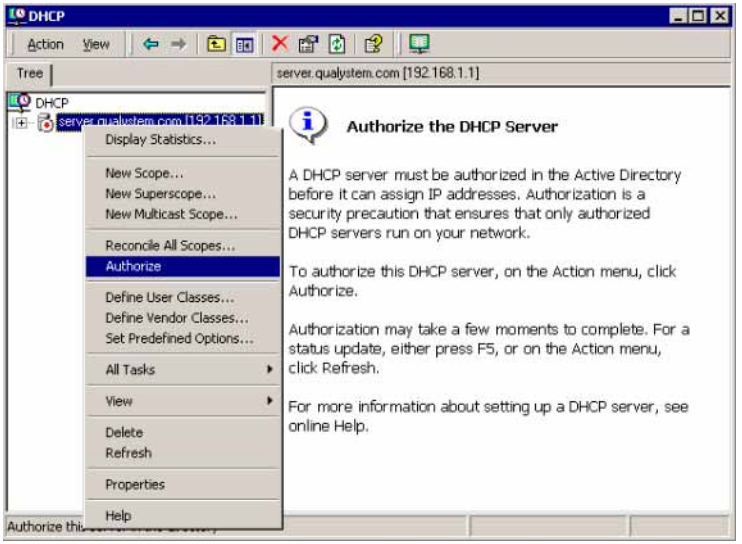

New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will active this scope later
< Back
Next >
Cancel

16 You now need to activate scope by selecting the option **Yes, I want to activate this scope now** then clicking **Next**.

(You can Activate/Deactivate the scope later with a right-click on the scope and selecting **Activate** or **Deactivate**.)

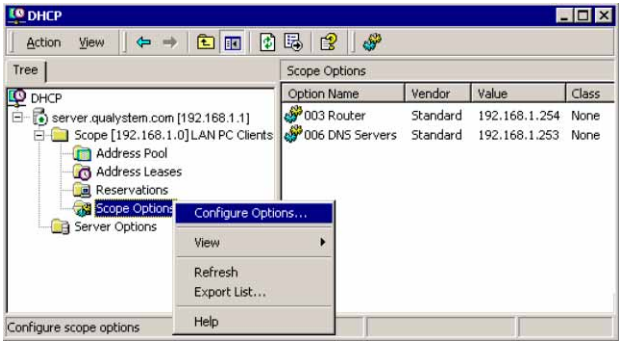
The following dialog will be displayed when the New Scope Wizard has successfully completed.

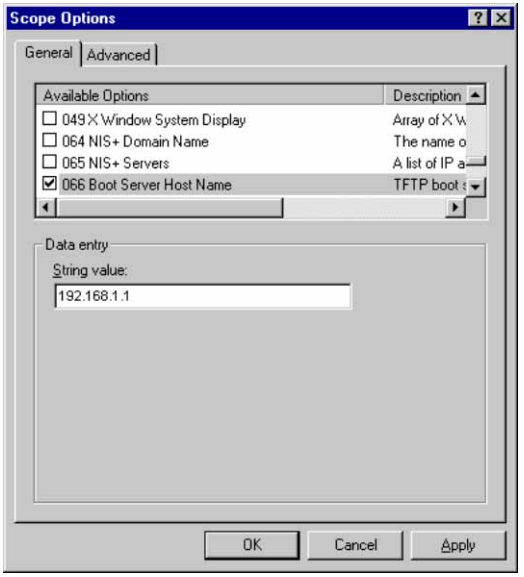
17 You now have to authorize the DHCP server. In the DHCP window, select the DHCP server and either right-click or from the **Action** menu select **Authorize**.


DHCP
Action
View
Tree
server.qualystem.com [192.168.1.1]
DHCP
Display Statistics...
New Scope...
New Superscope...
New Multicast Scope...
Reconcile All Scopes...
Authorize
Define User Classes...
Define Vendor Classes...
Set Predefined Options...
All Tasks
View
Delete
Refresh
Properties
Help
Authorize the DHCP Server
A DHCP server must be authorized in the Active Directory before it can assign IP addresses. Authorization is a security precaution that ensures that only authorized DHCP servers run on your network.
To authorize this DHCP server, on the Action menu, click Authorize.
Authorization may take a few moments to complete. For a status update, either press F5, or on the Action menu, click Refresh.
For more information about setting up a DHCP server, see online Help.

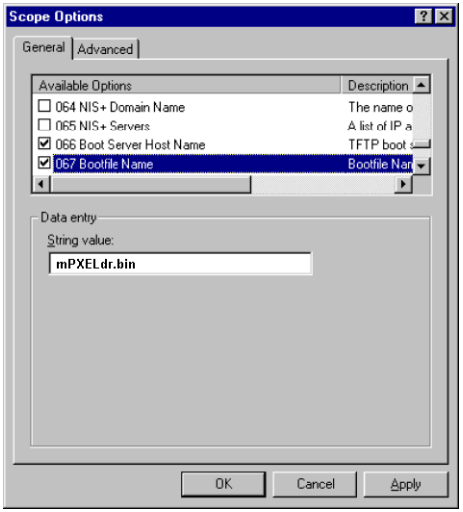
18 You may now have to close the DHCP window then open it again to see that the DHCP server is now running.

19 Open the **Scope Options** dialog by selecting the `Scope Options` folder in the tree-view pane of the DHCP window (or display the **Action** menu) and selecting **Configure Options**.





20 Scroll through the list box and check the option **066 Boot Server Host Name** check box. Enter your server's IP address in the **String Value** field. *Do not click OK yet!*



21 Scroll through the list and check the option **`067 Bootfile Name`** check box. Enter **`mPXELdr.bin`** in the **`String value`** field.

22 Click **`OK`** to accept the settings.

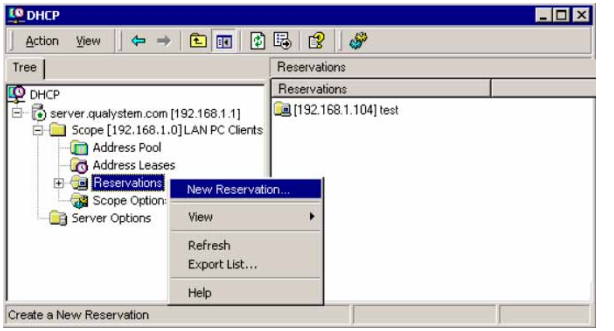
IMPORTANT: *Make sure that option* ***`060 Class ID`*** *is not present, or not checked, in* ***`Scope Options`*** *and in* ***`Server Options`****. Option* ***`060 Class ID`*** *is not present by default, but may be set if you previously installed a third-party PXE Server (Intel PXE PDK for example) on your server.*

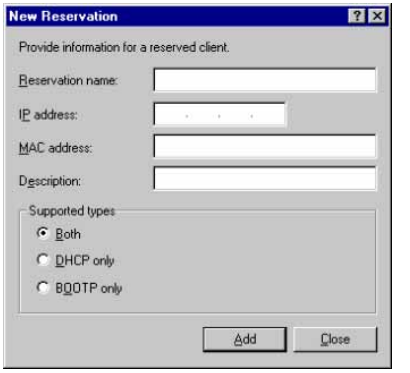
If option 60 exists and it is set to "PXEClient", you will need to configure a PXE Server for it to serve your clients with the boot file named `mPXELdr.bin`*. Note that some PXE servers do not allow per-client configuration. In this case you may want to set option 60 to an empty string for the MAC addresses corresponding to Neoware Image Manager clients. You would then use DHCP Reservations (see next section).*

DHCP Reservations

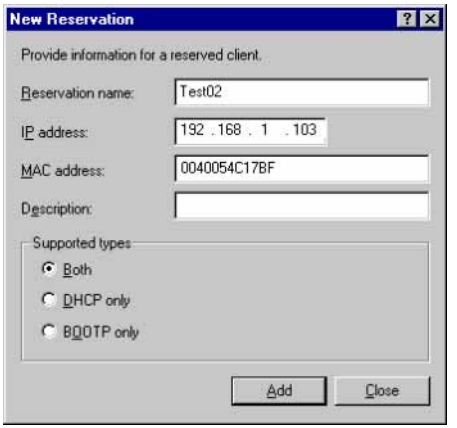
Even though DHCP assigns IP addresses dynamically on a first come, first served basis, using DHCP Reservations allows an IP address to be reserved for a specific client. An IP address can be matched with a MAC address to create a reservation. This allows DHCP to assign a "static" IP address. Furthermore, this allows each client to have a DHCP-provided specific host name.

1 Display the **New Reservation** dialog either by right-clicking on the `Reservations` folder in the tree-view pane of the **DHCP** Console and selecting **New Reservation...**, or by selecting `Reservation`, displaying the **Action** menu and selecting **New Reservation**.



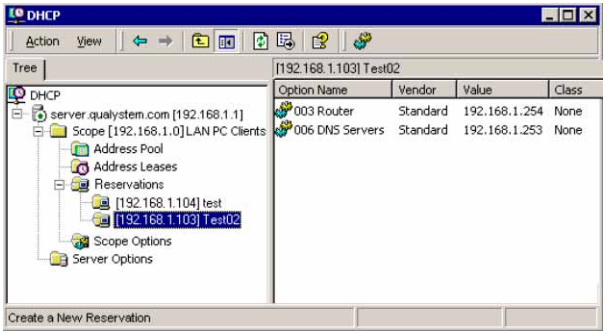


2 Enter a name for the reservation (just a "nickname"), the IP address you want to be assigned to the client, the client's MAC address, and an optional description.

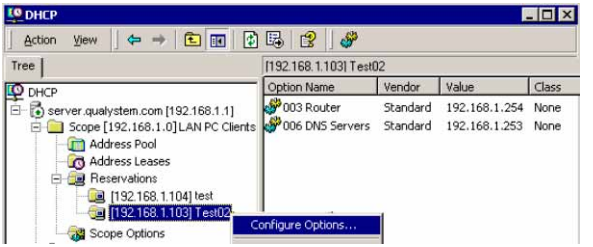


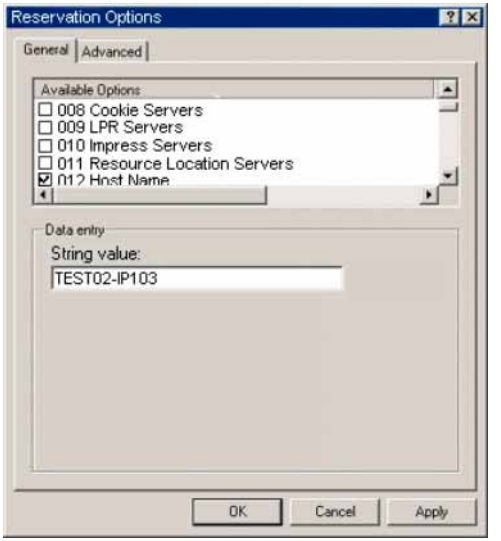
3 Keep the **Supported types** set to **Both** and click **OK**.

The newly created reservation will then appear under `Reservations` in the tree-view pane.



If you want to add a specific option to a reservation, for example a host name, you need to configure the options for that reservation. Right-click on the reservation you want to configure and select **Configure Options**.

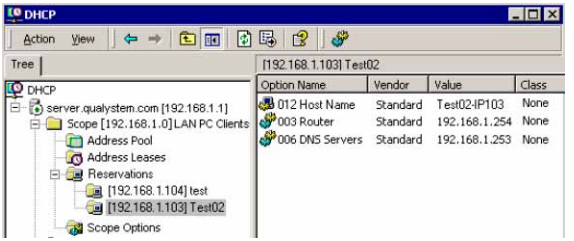




4 Scroll down to the particular option you want to set. To set the host name, select option 012.

Enter the desired value (`TEST02-IP103` in the example above) then click **OK**.

The option specific to that reservation will appear in the right pane when the reservation is selected in the tree-view pane.



Related Resources

Documents relating to MS Windows® DHCP server can be found at the following address:

`http://technet2.microsoft.com/windowsserver2008/en/servermanager/dhcpserver.mspx`

You can also refer to the following RFCs related to DHCP. RFCs can be browsed on the RFC web site: `http://www.rfc-editor.org`.

RFC 2131 Dynamic Host Configuration Protocol (protocol DHCP, obsoletes RFC 1541)

RFC 2132 DHCP Options and BOOTP Vendor Extensions

The following RFCs can help you understand how DHCP works with other services on your network:

RFC 951 The Bootstrap Protocol (BOOTP)

RFC 1534 Interoperability between DHCP and BOOTP

RFC 1542 Clarifications and extensions for Bootstrap protocol (BOOTP)

RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)

RFC 2241 DHCP Options for Novell Directory Services.

RFC 2242 Netware/IP Domain Name and Information.

APPENDIX D *DHCP Reference*

This appendix describes how clients locate the Neoware Image Manager server, and the DHCP options used.

How Clients Locate the Image Manager Server

At boot time, the Client station executes the mPXELdr code to locate an Image Manager Server to boot from. There are two ways to configure the server(s) that mPXELdr will attempt to contact. One is using the mPXELdr configuration file (described in the chapter “The mPXELdr Configuration File” on page 251). The other method involves a specific configuration option in the DHCP server, which is described in this appendix. Both methods are very similar and are designed to complement each other. To provide maximum configuration flexibility, refer also to the chapter “The mPXELdr Configuration File” on page 251.

The Neoware Image Manager server IP address and port number can be sent to a client by the DHCP server using DHCP option #132. This option must contain a comma-separated character string of IP addresses of servers to contact - optionally followed by a semicolon and a port number. If no port number is specified, the default NVDD port UDP 2184 will be used. It should be noted that the syntax of this option is strictly identical to that of the `NVDServers` option in the mPXELdr configuration file.

If an IP address that the client tries to contact is not running a Neoware Image Manager Server module on a corresponding port, or if the server running on that address and port cannot serve any

virtual disk to the client, the client tries to locate a running Neoware Image Manager server module by scanning the next IP address and port in the list sent in DHCP option #132. If the last server in the list does not answer (or if this list is empty), the client tries to connect to the IP address that is sent in `next-server` DHCP option #66 (field **siaddrr** of DHCP answer), using the default NVDD port UDP 2184.

The `next-server` option is used by PXE to identify the TFTP server that should send the network boot program `mPXELdr.bin` to the client.

Note: *If you do not want the client to boot off Neoware Image Manager virtual HDs served by the server that runs TFTP service, you have to end the value of DHCP option #132 with an exclamation mark (!). Refer to the chapter "The mPXELdr Configuration File" on page 251 and to the DHCP Options section for details.*

The DHCP option #60 should *NOT* be set in the DHCP replies. If you do set this option, please make sure that your PXE server will be able to serve the `mPXELdr.bin` file to your clients efficiently. If you do so, you may need to rename this file to `mPXELdr.0` (for example), depending on your PXE server.

dhcpd.conf File Example

The following is an example `dhcpd.conf` file for a TFTP server that has the IP address: 192.168.0.23, and NVDD servers that have the addresses: 192.168.0.4,192.168.0.9. (192.168.0.4 is tried first on port 10000 for client e100-01, then 192.168.0.9 is tried on port 2184, then 192.168.0.23 (TFTP server) is tried on port 2184).

```
option domain-name "neoware.com";
option domain-name-servers 192.168.0.12 ;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option subnet-mask 255.255.255.0;
ddns-update-style ad-hoc;
use-host-decl-names on;

# option 132 is used to store a comma separated list of
# IP addresses that the clients will scan to find
# a running nvdd server module
option option-132 code 132 = text;
```

```
default-lease-time -1;
max-lease-time 43200;

subnet 192.168.0.0 netmask 255.255.255.0 {
      host e100-01
      {
              next-server 192.168.0.23;
              hardware ethernet 00:00:39:3C:10:AB;
              fixed-address 192.168.0.75;
              filename "mPXELdr.bin";
               option option-132
"192.168.0.4:10000,192.168.0.9;" ;
      }
      host e100-02
      {
              next-server 192.168.0.23;
              hardware ethernet 00:00:39:18:01:AB;
              fixed-address 192.168.0.70;
              filename "mPXELdr.bin";
             option option-132 "192.168.0.4,192.168.0.9
:10000" ;
       }
```

Native DHCP Options

Image Manager takes into account the following DHCP options. This is especially useful when Microsoft Windows DHCP client has not been initialized yet. Also, if Microsoft Windows DHCP client is disabled (refer to the Windows DHCP Client section below), the following options will be used by Image Manager to set the correct TCP/IP configuration at boot time.

The following DHCP options are read in DHCP answers and automatically set in Neoware Image Manager Clients' Windows TCP/IP configuration at boot time:

Client IP Address: Assigned by DHCP.

Option #1: Client subnet mask.

Option #3: Default gateway.

Option #6: Domain Name Server (DNS).

Option #12: Computer host name. This value is used by Neoware Image Manager as the TCP/IP host name and also as the NetBIOS computer name (Windows computer name).

Option #44: WINS Server.

Option #132: Used by mPXELdr to get a list of server IP addresses (optionally followed by a colon (:) and a port number. If no colon and port number is specified, standard NVD port UDP 2184 is used) that can respond to NVDD requests. mPXELdr will try each of the IP addresses listed in this option, in the order in which they appear, until it finds a server that answers and that actually serves at least one bootable virtual drive to the client. This IP address (and optionally this port) is used afterwards as the IP address for the Neoware Image Manager server for this client. If this DHCP option is not specified or is empty, or if none of the server IP addresses sent by this option answers to `mPXELdr` requests, mPXELdr then tries to use the IP address of the TFTP server that sent mPXELdr to the client, as the NVDD server, unless the list ends with an exclamation mark (!) character (in which case it will then loop to the first server in the list). The actual list of server IP addresses that mPXELdr tries to contact is in the following order:

```
<IP addresses in DHCP Option#132>, next-
server (DHCP Option #66)
```

If you do not end the list in DHCP option #132 with an exclamation mark (!), remember that mPXELdr will try to mount virtual drives hosted on the server that provided TFTP service.

By default, the `BDRUPD.sys` driver reads the DHCP options and tries to identify them. If the option is a known one, it is processed (i.e. the

corresponding information is set in Windows TCP/IP settings). In order for the `BDRUPD.sys` driver to handle new options, a registry key exists under BDRUPD as follows:

`HKLM\SYSTEM\CurrentControlSet\Services\BDRUPD\DHCPTags`

Note: NVDDTags (options sent by the NVDD server) are also processed by BDRUPD. *These option definitions are found under the key:*

`HKLM\SYSTEM\CurrentControlSet\Services\BDRUPD\NVDDTags`

The NVDDTags options will be handled by BDRUPD with exactly the same process as for the DHCPTags options. You can then use the following description for NVDDTags option settings as well as for DHCPTags option settings.

Note that if a DHCPTag option and a NVDDTag option have the same target, the NVDDTag will have the highest priority and will overwrite the DHCPTag function.

Under this key, a new subkey is created for each option that `BDRUPD.sys` can process. The subkey name must be the decimal option number. Each option subkey must contain the following values:

Type : REG_DWORD. Indicates the type of data transmitted by DHCP. It can have one of the following values:

- **0** the source data is an IP address or list of IP addresses.
- **1** the source data is a string.
- **2** the source data is an integer.
- **3** the source data is a time value.
- **4** the target data must be set to 0 (DWORD) or "empty string" (REG_SZ, REG_MULTI_SZ, REG_EXPAND_SZ). The source data is ignored.

RegType : Indicates the type of the value to set in the registry. This, combined with **Type** gives BDRUPD the conversion to

perform before continuing the process. The actual value is useless, BDRUPD uses the ***type*** of the **RegType** value as the type of the value(s) it will write to the keys.

Target : REG_MULTI_SZ. Contains couples of path + value to modify. The data given by the DHCP option value will be set at each path / value set in this list. The **Target** value must contain an even number of strings. The first string is a path to a key in the registry. The second string is the name of the value to modify in the key whose path is stored in the first string. The third string is a path to a key in the registry. The fourth string is the name of the value to modify in the key whose path is stored in the third string, etc. For example, if the first string contains `\Registry\Machine\SOFTWARE\Neoware` and the second string contains `Test`, BDRUPD will update the value named `Test` in the key: `HKEY_LOCAL_MACHINE\SOFTWARE\Neoware`.

The process is as follows. BDRUPD gets a DHCP option value (or an NVDDTag option value). It searches the corresponding subkey in its registry parameters. If it exists, it reads the Type and RegType to perform a conversion (if required). Then it reads the targets and inserts the converted data to each location.

Optional Subkeys & Values

If an option needs multiple to be set at multiple places in the registry, it is possible to add a new subkey to the option key. Subkeys are numeric (starting at 1 and incrementing). BDRUPD will try to locate these keys in order until it fails to find one. Each subkey has the same structure as the main option key, except that it cannot have a subkey. BDRUPD will process its content as described above.

When an option must be set only if a condition is validated, the user can use the "If" and "IfNot" values, at the same level as the RegType, Type and Target values.

If REG_SZ. Contains a registry path to a DWORD value. This value is read by BDRUPD. If it is *not* zero the option is processed: the Target is written with the value of the option or emptied if Type=4. Otherwise this key is ignored.

IfNot REG_SZ. Contains a registry path to a DWORD value. This value is read by BDRUPD. If it is zero the option is processed: the Target is written with the value of the option or emptied if Type=4. Otherwise this key is ignored.

Note that if a key is ignored, BDRUPD will not abandon this option. It will continue searching for applicable conversions in the subkeys, if any.

As it may be difficult to write full paths for **Target**, and some locations may not be known (hardware dependent IDs, etc), the following keywords have been set to help create coherent targets:

%INTERFACE_ID% This keyword replaces the internal identification number of a network card. BDRUPD, when finding this keyword, will replace it with the ID of the network card it has been assigned to use at installation time. If multiple NICs have been defined, BDRUPD will update the settings for all of them.

%ACTIVE_NIC% means the information will be set at two locations:

```
%SERVICES%\Tcpip\Parameters\Interfaces\%INTERFACE_ID%
%SERVICES%\%INTERFACE_ID%\Parameters\Tcpip
```

%SERVICES% means the following location:

```
\Registry\Machine\System\CurrentControlSet\Services
```

%CONTROL% means the following location:

```
\Registry\Machine\System\CurrentControlSet\Control
```

Examples

The DHCP option 1 provides the client's subnet mask. This information must be set in the active network card's TCP/IP configuration, under the "SubnetMask" value. Also, if MS DHCP client is enabled by BDRUPD, this option must also be set as "DhcpSubnetMask".

The following illustrates how BDRUPD is configured to process this correctly:

```
HKLM/System/CurrentControlSet/Services
    BDRUPD (key)
    DHCPTags (key)
        1 (key)
        Type (REG_DWORD) : 0
        RegType (REG_MULTI_SZ) : ""
        Target (REG_MULTI_SZ) : "%ActiveNIC% SubnetMask"

        1 (subkey)
        Type (REG_DWORD) : 0
        RegType (REG_SZ) : ""
        Target (REG_MULTI_SZ) : "%ActiveNIC% DhcpSubnetMask"
        If (REG_SZ) : "\Registry\Machine\System\CurrentCon-
trolSet\Services\BDRUPD\SetDHCP"
```

This way, the option value is written to the proper value (SubnetMask) and optionally to the second one (DhcpSubnetMask) only if MS DHCP client is activated by BDRUPD (through the BDRUPD flag "SetDHCP").

Changing the Client's Name with NVDD Tags

```
HKLM/System/CurrentControlSet/Services
    BDRUPD (key)
    NVDDTags (key)
        1 (key)
        Type (REG_DWORD) : 1
        RegType (REG_SZ) : ""
        Target (REG_MULTI_SZ) :"%CONTROL%\ComputerName\Comput-
erName"
                                "ComputerName"
                                "%SERVICES%\TcpIp\Parameters"
                                "HostName"
```

Removing a Value

The DHCP option 6 is used to set the DNS list. These data must be set in the registry value "NameServer" if Microsoft Windows DHCP client is NOT activated. If it is activated, the "NameServer" entry must be set to an empty string, and the data must be set to the DhcpNameServer value instead. Here is how BDRUPD is configured to achieve this:

```
HKLM/System/CurrentControlSet/Services
    BDRUPD (key)
    DHCPTags (key)
        6 (key)
        Type (REG_DWORD) : 4
        RegType (REG_SZ) : ""
        Target (REG_MULTI_SZ) : "%ACTIVE_NIC% NameServer"
        If (REG_SZ) : "\Registry\Machine\System\CurrentCon-
trolSet\Services\BDRUPD\SetDHCP"

        1 (subkey)
        Type (REG_DWORD) : 0
        RegType (REG_SZ) : ""
        Target (REG_MULTI_SZ) : "%ACTIVE_NIC% DhcpNameServer"
        If (REG_SZ) : "\Registry\Machine\System\CurrentCon-
trolSet\Services\BDRUPD\SetDHCP"

        2 (subkey)
        Type (REG_DWORD) : 0
        RegType (REG_SZ) : ""
        Target (REG_MULTI_SZ) : "%ACTIVE_NIC% NameServer"
        If (REG_SZ) : "\Registry\Machine\System\CurrentCon-
trolSet\Services\BDRUPD\SetDHCP"
```

Setting a Timeout Value

The following example uses a custom DHCP option (129) to set a timeout value:

```
HKLM/System/CurrentControlSet/Services
    BDRUPD
    DHCPTags
        129
        Type (REG_DWORD) : 2
        RegType (REG_DWORD) : ""
        Target (REG_MULTI_SZ) : "%SERVICES%\MyService\Parame-
ters"

                                        "Timeout"
```

NetBIOS Name for Clients

The NetBIOS name of a Neoware Image Manager client is set to Client Host Name, as set by NVD name (see the *Client Naming* section), or by DHCP replies. This section deals only with the case when the client name is set only by DHCP option #12.

The host name can be set with DHCP option #12, also known as `Client Host Name` or `Host Name`.

Setting a host name for a specific client usually implies that there is a one-to-one relationship between a host name and the corresponding MAC address for a client.

If you use Windows NT/2000 DHCP Server, you may refer to the section “DHCP Reservations” on page 312.

If you use a different DHCP server, refer to your DHCP server documentation, in particular check if `use-host-decl-names` can be set to `on`.

The NetBIOS name cannot be set directly by DHCP. Neoware Image Manager client uses Internet Host Name (DHCP option #12) as the client NetBIOS name. Setting DHCP server to include the option Client Host Name in its answers usually implies that the DHCP server uses static entries (also known as DHCP Reservations). When a DHCP server uses static entries, a unique IP address is assigned to a unique MAC address and a Client Host Name can also be set.

If the NVDD server does not provide a client name and the DHCP option Client Host Name (DHCP option #12) is not set in DHCP replies, Neoware Image Manager client initializes the client NetBIOS name to a string formed with `H<ClientMacAddress>`. For example, a client with the MAC address `001122334455` will have `H001122334455` as its NetBIOS name if DHCP replies do not include option #12 for this client and Image Manager does not have a specific entry for this particular client.

Windows DHCP Client

In previous versions of Neoware Image Manager, the client's IP settings were set as "statically assigned address" (even if the address was provided by the DHCP server), and set by the Neoware Image Manager integrated DHCP client. This behaviour could lead to issues with some DHCP servers where the lease was not regularly renewed.

To prevent this situation from occurring, the Windows DHCP client is now used by default. This means that clients will be set automatically to retrieve their IP addresses from the DHCP server, and will renew their leases automatically.

This configuration performs better in existing networks and is more compliant with the DHCP requirements. However, if you want to disable Windows DHCP and revert to the previous behaviour (to use the Neoware Image Manager integrated DHCP client instead), you can edit the following registry key:

Key: `HKLM/System/CurrentControlSet/Services/BDRUPD`

Value: `SetDHCP (DWORD)`

Set it to "`0`" to disable DHCP, or "`1`" to enable it.

APPENDIX E

Configuring NVDD as a Windows Service

This appendix describes how to configure the Image Manager server as a Windows service.

Introduction

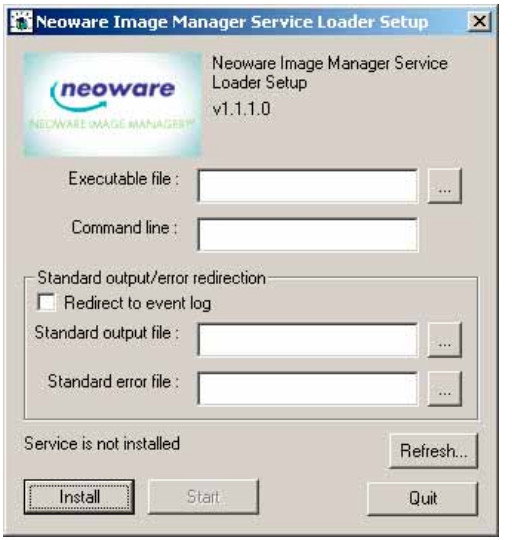
The Neoware Service Loader is a utility that enables execution of the Image Manager server as a service on Windows NT/2000/XP/2003 boxes that run the Image Manager server module `nvdd`.

Installation Procedure

1. In order to install Neoware Image Manager Server as a service, you have to run the "Neoware Image Manager Server Service" utility. Usually you can do this from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Image Manager Server Service**.

   If necessary (for instance if you did not perform a **Server** or **Server + Console** installation type on your server machine), copy the file `SrvcLoader.exe` and `SrvcLoaderSetup.exe` into the directory where the NVDD server module `nvdd.exe` is located. These files are usually found in the `Server/Windows` directory of the Neoware Image Manager software distribution package.

2. Launch Neoware Image Manager Server Service (`SrvcLoaderSetup.exe`). The following dialog will be displayed.



3 In the **Executable file** field, enter the directory path and filename of the Neoware Image Manager server module (usually `nvdd.exe`). You can click the **...** button to browse for the file.

4 The **Command line** field enables you to specify arguments that are to be sent to the Image Manager server module. These are usually in the form:

`-c nvdd.<image filename>.conf -n`

For example:

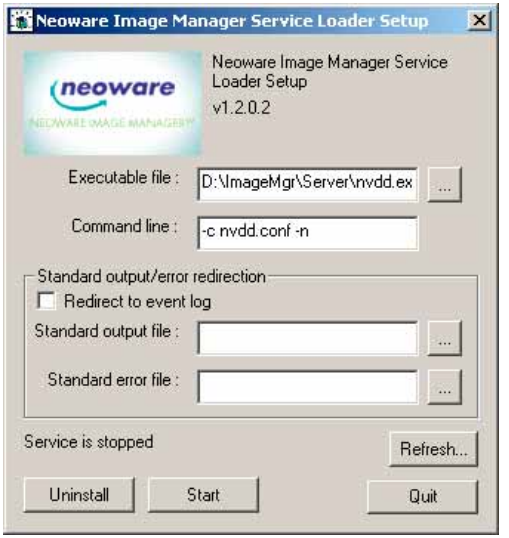
`-c nvdd.disk.bin.conf -n`

`-n` is usually specified when nvdd is run as a service, as it allows the service to be launched even if there is a `.lock` file (which can exist after a power failure, for example).

Refer to the appendix "NVDD Reference" on page 337 for information on the arguments that can be used.

5 You can check the **Redirect to event log** box so that Image Manager server messages are redirected to the standard Windows event log.

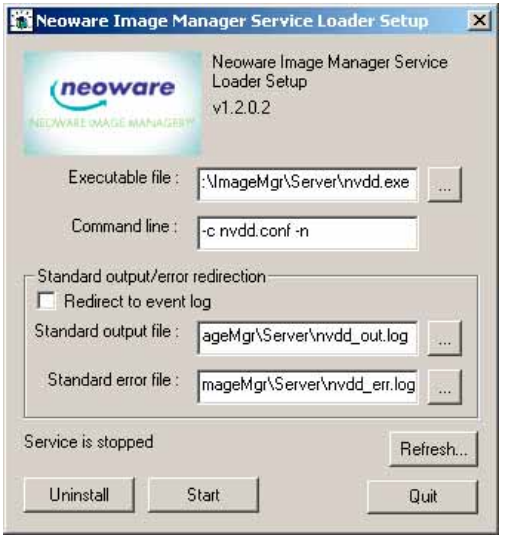
The following illustration shows the typical entries for configuring the Image Manager server to be run as a Windows service.



6 If you want Image Manager server messages to be stored in different log files, uncheck the **Redirect to event log** box and specify valid paths for the **Standard output file** (`stdout`) and **Standard error file** (`stderr`). Be aware that these files may use up a lot of disk space on the server's hard disk. You will not be able to open these files until the `nvdd` server module is stopped. If no file names are specified then the NVDD messages will not be stored anywhere. Note that these files are not needed for the execution of Image Manager server.

If no path is specified for these log files, they will be created in the `SYSTEM32` directory under the `Windows` directory (usually `C:\WINDOWS\SYSTEM32` or `C:\WINNT\SYSTEM32`). It is highly recommended that you specify a complete (absolute) path for these files.

The following illustration shows typical entries for redirecting server messages to log files.



7 When all the required settings have been specified, click the **Install** button.

Neoware Service Loader will install and configure `nvdd` to work as a service. You can then Start and Stop the service using the Neoware Service Loader Setup dialog `SrvcLoaderSetup.exe` or the Windows **Services** applet in **Administrative Tools**.

Using NVDD as a Service

When `nvdd` is installed as a service, Neoware Service Loader Setup allows you to start or stop it.

1. Run Neoware Service Loader Setup, either from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Image Manager Server Service**, or by navigating the file system:

   ```
   Program Files/Neoware/Image_Manager_4.6/Server/Windows/SrvcLoaderSetup.exe.
   ```

2. Click the **Start** button to start the service.

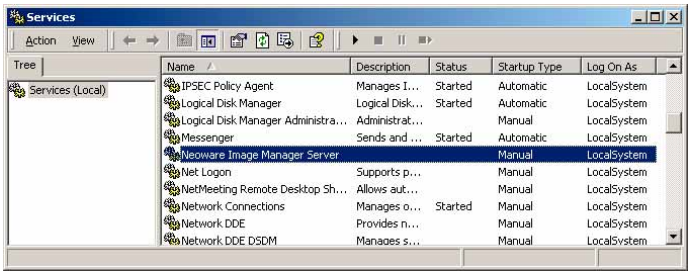
The current status of the service is displayed above the **Start** button. Clicking **Refresh** will update the service status if it has changed.

You can **Quit** Neoware Service Loader Setup while the service is running; it will not stop the service itself. You can relaunch it whenever you need to control the NVDD service. The service can also be stopped using Neoware Service Loader Setup; the **Start** button becomes a **Stop** button when the service is running.

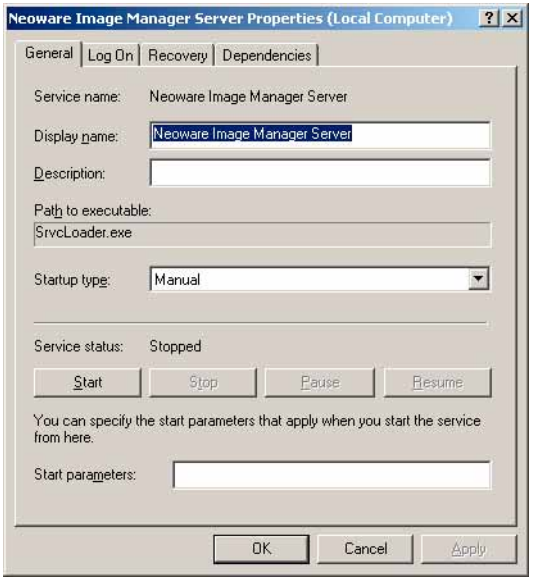
Configuring NVDD Service Options

The newly installed service is configured to be run manually. This means you can start or stop it using the Services interface of Windows NT/2000/XP/2003. You can also configure it to be launched automatically at server startup by using this interface.

1. In the Windows **Control Panel**, select **Administrative Tools** then **Services**.

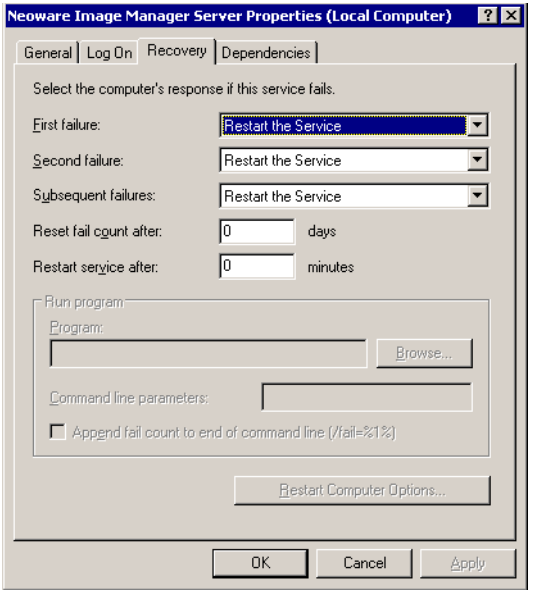


2 Double-click on the **Neoware Image Manager Server** entry to display the service properties.



This dialog allows you to control the behaviour of the service. Usually you will select **Automatic** as the **Startup** type, so that the NVDD service runs automatically when the server box is switched on, even if no user actually launched the `nvdd` server module.

You can also configure the **Recovery** options for the service. For example, if you want the service to restart automatically in case of failure, you would use the following configuration:



Uninstalling the Service

To uninstall the NVDD service, just click the **Uninstall** button in the Neoware Service Loader Setup dialog. This will stop the service if it is running, and uninstall it from the system.

Changing Service Settings

To change the settings for the NVDD service:

1. Run Neoware Service Loader Setup, either from the **Start** menu by selecting **Programs** > **Neoware** > **Image Manager** > **Tools** > **Neoware Image Manager Server Service**, or by navigating the file system:

   `Program Files/Neoware/Image_Manager_4.6/Server/Windows/SrvcLoaderSetup.exe.`

2. If the **Stop** button is displayed, click it.
3. Change the settings in the dialog.
4. Click the **Start** button.

APPENDIX F

NVDD Reference

This appendix describes the command line options that can be used when launching the nvdd server module.

Introduction

The Neoware Image Manager server module `nvdd` is the main Network Virtual Disk (nvd) daemon. It reads a configuration file then shares hard disk images and virtual volumes among specified clients on the network using the nvd protocol. There are several command line options that can be used when launching the `nvdd` server module. These are described below.

Command Syntax

The syntax for the `nvdd` server module command is as follows:

```
nvdd [-v <loglevel>][-p <port_number>][-c <config_file>]
[-l <log_file>][-n]
```

Verbose Mode

`-v all¦proto¦io¦conf¦timo`

This command line option enables you to display various messages about `nvdd` operation.

`all` Print all messages.

`proto` Print messages relating to the code that has been executed in `nvdd`.

`io` Print messages relating to network and disk inputs/outputs.

`conf` Print messages relating to initialization and configuration file parsing.

`timo` Print messages relating to timeouts.

Note that if `all` or `timo` is specified, `nvdd` will display all time-out messages, including those indicating that `nvdd` is waiting for communication. The message `checking for idle clients` will be displayed frequently. This is *not* an error message, it is the normal behaviour of `nvdd` when no client is communicating with it.

Port Number

`-p <port_number>`

This command line option enables you to specify a different port number for `nvdd` to use, overriding the one specified in the configuration file. This option should be used for tests only. If NVD port in the configuration file is different from the command line parameter specified with the `-p` option, the port number specified in the configuration file will be used again after that file has been reloaded by Neoware Image manager Console or the NVDDAdmin tool.

Configuration File

`-c <config_file>`

This command line option will make `nvdd` read the specified configuration file. When this is not specified, `nvdd` will look for a file named `nvdd.conf` in the current directory.

Log File

`-l <log_file>`

This command line option will make the server write all screen messages into the specified file as well as to the console, enabling you to keep a record of server activity.

No Lock File Check

`-n`

This command line option will prevent the server from checking for the presence of the `.LOCK` file before trying to create it. This option has been added to improve support of power failures and startup

scripts or processes. In the case of a server having a power failure, nvdd will not be shutdown cleanly and the .LOCK file will remain, preventing nvdd from being launched automatically, at least while the .LOCK file has not been removed.

Users should use this option only in startup scripts (i.e. scripts that are launched when the server computer is starting). Users that use Linux/FreeBSD servers are encouraged not to use this option but set scripts that would remove the .LOCK file only if the startup script is launched by the startup process of the server OS.

For more details about .LOCK files, refer to the section “The nvdd.conf.LOCK File” on page 348.

APPENDIX G *NVD.SYS Reference*

This appendix describes the parameters that can be set in the registry entry for the `NVD.SYS` driver.

Introduction

At the client side, `NVD.SYS` is the Neoware Image Manager driver in charge of communications with the Image Manager server. This appendix describes the parameters that can be set in the registry entry for the driver, which is located in:

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Nvd
```

Parameters

IP Address

`ip_address`

This DWORD value specifies the address of the Neoware Image Manager server used in this session. The value is set at boot time. Changing this setting in the image will not change client behaviour.

Port Number

`Port`

This DWORD value specifies the number of the communication port to use with NVD protocol. This must be the same as the one used by the server. Changing this setting in the image will not change client behaviour.

Sectors Per Request `sector_per_request`

This DWORD value defines the maximum number of sectors asked at one time by the client in each read/write operation. The allowed values are: 32, 64 or 128 (default).

This value can be set to less than 128 to fine tune the flow of data transmission between client and server. This has been proven to be useful (rarely) with some GigaEthernet/100BaseT switches for which the buffers dedicated to GigaEthernet packets were too small. When the Neoware Image Manager server was connected to one of the GigaEthernet ports, some packets were overwritten before having been dispatched to the Ethernet 100 ports, resulting in a significant decrease in performance.

Shutdown Timeout `shutdown_timeout`

This DWORD value specifies the time, in seconds, during which disk requests can be transmitted to Neoware Image Manager virtual disk drives after the shutdown order has been received by the drivers of the virtual disks. In other words, this controls the delay between the shutdown order being received and the moment the virtual disks are actually shut down. If you experience problems at shutdown, especially if Windows hangs, you may need to increase this value.

Boot Volume `boot_vol`

This DWORD value specifies the internal ID of the volume to use as the boot volume. The value is set at boot time. Changing this setting in the image will not change client behaviour.

Cache Size `cachesize`

This DWORD value specifies the size, in sectors, of the memory to use as cache (not currently used).

Network Interfaces Binding

`nic_list`

This REG_MULTI_SZ value contains indexes of network cards that are used by Image Manager as Virtual Drive controllers. The index numbers are set by Client Builder when the user selects the interfaces to be used as Virtual Disk controllers, or when UbiBoot Inserter adds the support for a network card into the image.

Users should never edit this field manually as it could result in images becoming non-bootable.

Domain Credentials Handling

`domain_membership`

Default: 0

This DWORD value specifies whether the domain credentials have to be transferred from the NVDD server at boot time and to the NVDD server at shutdown time. A value of 1 enables domain credential transfer from and to the NVDD server. A 0 value disables it.

APPENDIX H

File Transfer

This appendix describes issues relating to the file transfer capabilities of Image Manager.

Introduction

Image Manager uses two file transfer protocols:

- The file transfer protocol NVDFTP is integrated in the NVD protocol (the HDD emulation protocol), and is used in particular to transfer the Domain Credentials at boot and shutdown time.
- A file transfer protocol is integrated in the NVDAdmin protocol (used to remote control NVDD servers), and is used in particular to get a remote `nvdd.conf` file or to deploy CVol files to a remote server.

Root Folder for File Transfers

Both file transfer protocols can transfer files only from and into the folder specified by the `client_files_dir` parameter in the `nvdd` configuration file. This parameter can also be set in the Image Manager Console, on the **Directories** tab of the **Generic Properties** dialog.

By default, the root folder for file transfer files is the folder where the NVDD server module resides. We recommend that you change this setting for security reasons. If you do not change this setting,

anyone who knows how to transfer files using NVDFTP or NVDAdmin could copy or replace the files in this folder, in particular your license file, your configuration files, your images etc.

In order to add some security to NVDAdmin protocol, we recommend that you set a password on the server side (using the `NvddPasswd` tool - refer to the section “Password for Remote Administration” on page 210 for details). Then, any file transfers using the NVDadmin protocol will require the user to enter a password before files can be transferred.

The root folder has been set for security considerations. This has some implications. In particular, files created by NVDAdmin, such as the image files that client builder creates, will be created in this root folder. You may need to tune the configuration file in order to reflect this situation.

Note that the configuration file currently in use is copied to a file named `current.<configuration file name>` *in the file transfer root folder.* All standard NVDAdmin operations on the current configuration file are actually performed on the `current.<configuration file name>` file. When `nvdd` shuts down (or when the configuration file is reloaded), the configuration file is copied back to where it was loaded from. Users should never edit or modify the file `current.<configuration file name>` in the file transfer root folder while Image Manager server is up and running, as this could cause unpredictable behaviour.

APPENDIX I

NVDD Temporary Files

This appendix describes issues relating to temporary files created by the nvdd process.

The NVDD Configuration File

When `nvdd` is launched it creates a temporary copy of the configuration file in the directory specified by the `client_files_dir` parameter in the `nvdd` configuration file, and uses this copy to work with. The temporary configuration file copy has the same name as the original configuration file but has the prefix `current`.

For example, if `nvdd` is launched with the following parameters:

```
nvdd –c nvdd.disk0.vol.conf
```

it will create the file named

```
current.nvdd.disk0.vol.conf
```

In what follows, we will assume that `nvdd` was launched to use the nvdd.conf configuration, and that the current configuration file is named `current.nvdd.conf`.

Any changes made to the configuration, using the remote Console for example, will be applied to the `current.nvdd.conf` file. When `nvdd` is shut down, the changes stored in `current.nvdd.conf` will be merged into the original configuration file and (assuming the merge was successful) the `current.nvdd.conf` file will be deleted.

If the NVDD server crashes, due to a power failure for example, the temporary file `current.nvdd.conf` will still remain in the directory specified by `client_files_dir`. The next time `nvdd` is launched it will copy any files prefixed with `current.` into a subdirectory of the `client_files_dir` called `restoredfiles`, and add a timestamp to the end of each filename. This makes it possible for an administrator to recover configuration files that include changes that have not yet been applied.

The nvdd.conf.LOCK File

In order to prevent conflicts, a configuration file can only be opened by one `nvdd` process at a time. When `nvdd` is launched it creates a file with the same name as the configuration file but appended by `.LOCK`. This file will be placed in the same directory as the configuration file.

When `nvdd` is launched again, it checks that there is no `.LOCK` file that corresponds to the configuration file it is attempting to use. If there is a `.LOCK` file then `nvdd` will refuse to launch.

If the NVDD server crashes, due to a power failure for example, the `.LOCK` file will still remain. You must manually delete or rename the `.LOCK` file in order to be able to launch `nvdd`.

CAUTION: *Before you actually delete the `.LOCK` file and launch `nvdd` with the related configuration file, ensure that no other `nvdd` process is actually using the locked configuration file, otherwise you may corrupt your configuration file as well as your server execution.*

USER_REP Files

Client names set by the NVD protocol are stored in the configuration file. In certain conditions these names can be changed from the client side. In order to preserve the integrity of the configuration file and to allow two clients to change their names at the same time, the data relating to changed client names are temporarily stored in a file

named USER_REP.<*configuration file name*>. This file is located in the directory where the NVDD server resides. You can also specify the directory in the Neoware Image Manager Console using the **Client files folder** option (select **Generic options** in the **Tools** menu, then click the **Directories** tab).

When nvdd is stopped or restarted, or when the configuration file is reloaded (through the console or NVDDAdmin for instance), the USER_REP.<*configuration file name*> file is merged into the original configuration file and then deleted.

If the NVDD server crashes, due to a power failure for example, the USER_REP.<*configuration file name*> file will still remain. The next time nvdd is launched it will copy the file into a subdirectory of the client_files_dir called restoredfiles, and add a timestamp to the end of each filename. This makes it possible for an administrator to recover USER_REP* files and process them.

As the restoredfiles folder also contains the restored configuration files, with the same timestamp, it is easy for the administrator to know which USER_REP file corresponds to which configuration file.

How to Retrieve Restored Files

If the NVDD server crashes, the next time it is launched it will save found temporary files in a directory called restoredfiles, a subdirectory of client_files_dir.

Files found in the directory restoredfiles are the currently used configuration file and, optionally, the corresponding USER_REP file. Both will have the same timestamp to ensure they are not confused with other versions.

To restore the configuration file and integrate the USER_REP information into it, you must:

- use the restored configuration file when launching the server (possibly by copying/renaming it in the NVDD server folder)

- place (copy) the USER_REP file and give it the name USER_REP.<*configuration file name*>.

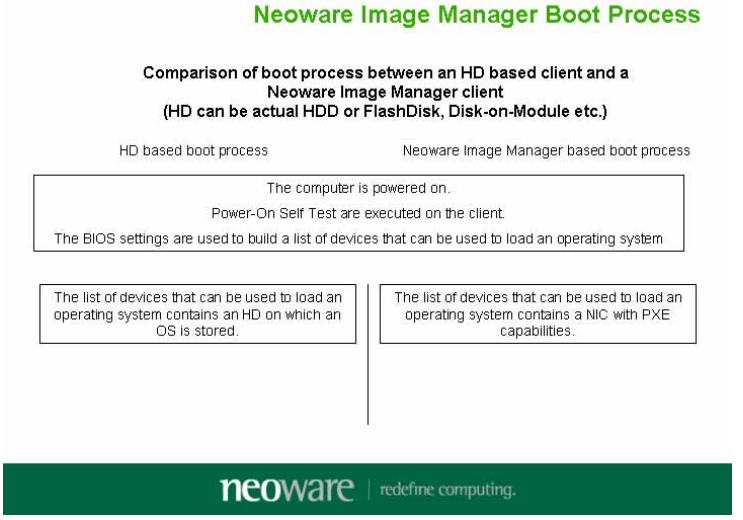
When you close or restart the server, or reload the configuration file using the appropriate Console button, the data inside the USER_REP file will be processed as usual, and the USER_REP file will be deleted. The configuration will then contain the updated information.

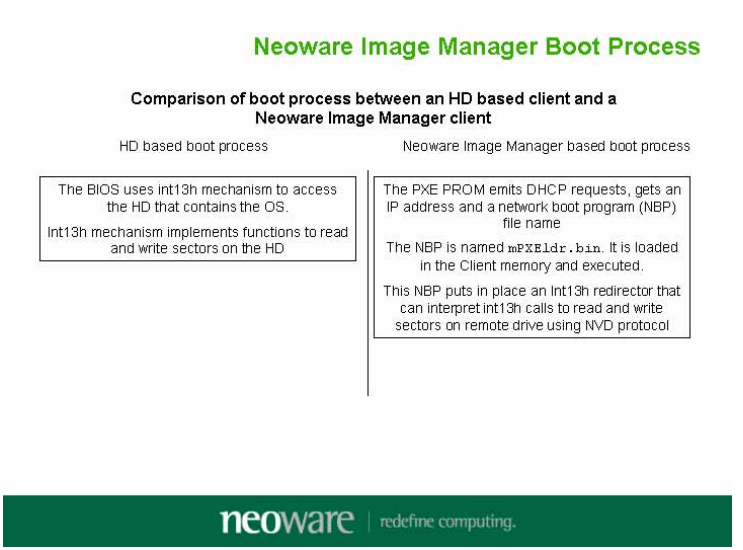
APPENDIX J

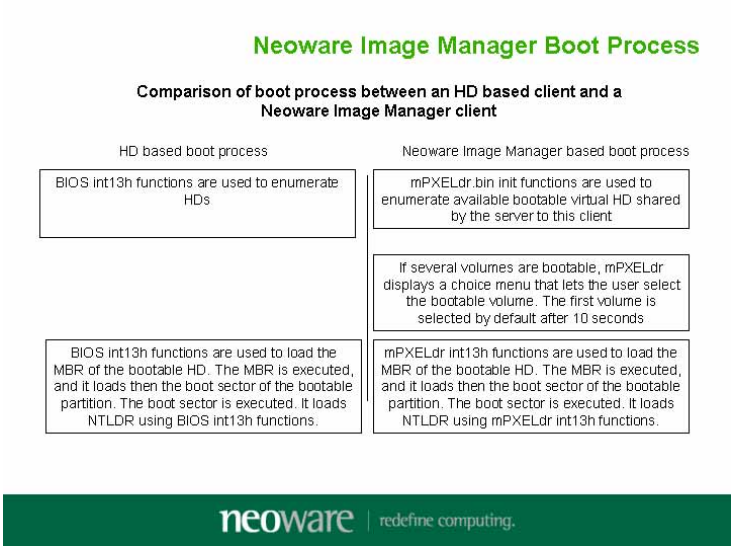
Boot Process Comparison

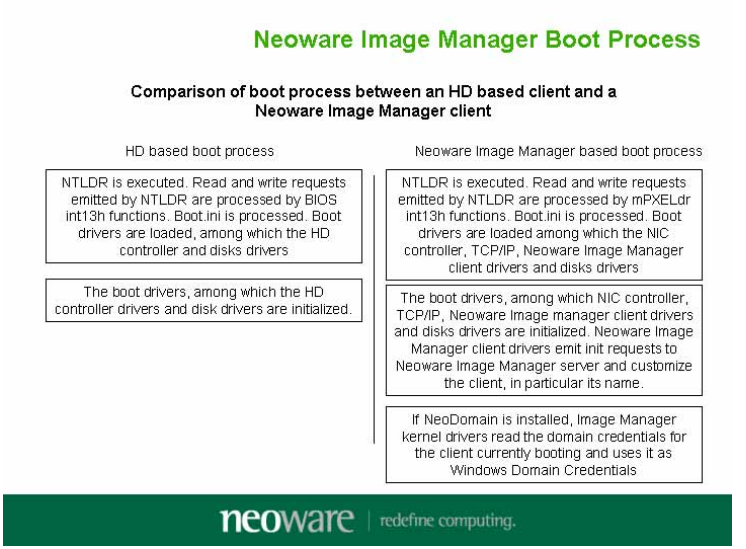
This appendix provides a side-by-side comparison between a HDD-based boot process and the Neoware Image Manager based boot process.

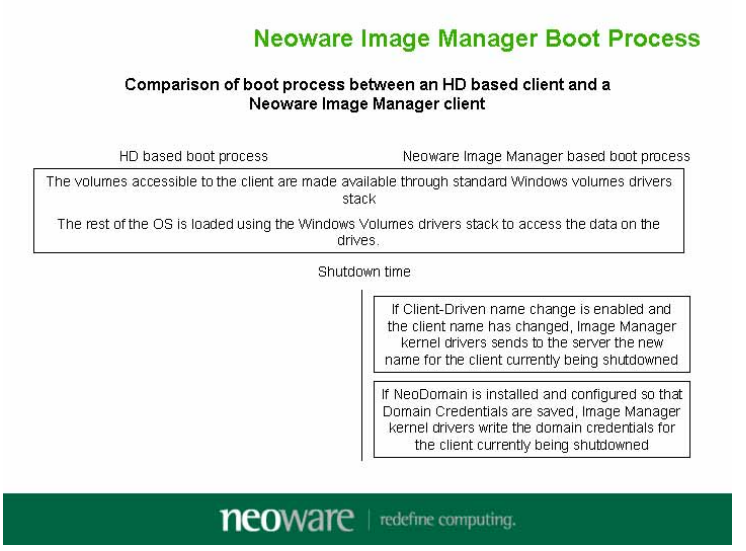
The following illustrations contain a side-by-side comparison between a HDD-based boot process and the Neoware Image Manager-based boot process.


Neoware Image Manager Boot Process
Comparison of boot process between an HD based client and a Neoware Image Manager client (HD can be actual HDD or FlashDisk, Disk-on-Module etc.)
HD based boot process
Neoware Image Manager based boot process
The computer is powered on.
Power-On Self Test are executed on the client.
The BIOS settings are used to build a list of devices that can be used to load an operating system
The list of devices that can be used to load an operating system contains an HD on which an OS is stored.
The list of devices that can be used to load an operating system contains a NIC with PXE capabilities.
neoware | redefine computing.


Neoware Image Manager Boot Process
Comparison of boot process between an HD based client and a Neoware Image Manager client
HD based boot process
Neoware Image Manager based boot process
The BIOS uses int13h mechanism to access the HD that contains the OS.
Int13h mechanism implements functions to read and write sectors on the HD
The PXE PROM emits DHCP requests, gets an IP address and a network boot program (NBP) file name
The NBP is named mPXEldr.bin. It is loaded in the Client memory and executed.
This NBP puts in place an Int13h redirector that can interpret int13h calls to read and write sectors on remote drive using NVD protocol
neoware
redefine computing.


Neoware Image Manager Boot Process
Comparison of boot process between an HD based client and a Neoware Image Manager client
HD based boot process
Neoware Image Manager based boot process
BIOS int13h functions are used to enumerate HDs
mPXELdr.bin init functions are used to enumerate available bootable virtual HD shared by the server to this client
If several volumes are bootable, mPXELdr displays a choice menu that lets the user select the bootable volume. The first volume is selected by default after 10 seconds
BIOS int13h functions are used to load the MBR of the bootable HD. The MBR is executed, and it loads then the boot sector of the bootable partition. The boot sector is executed. It loads NTLDR using BIOS int13h functions.
mPXELdr int13h functions are used to load the MBR of the bootable HD. The MBR is executed, and it loads then the boot sector of the bootable partition. The boot sector is executed. It loads NTLDR using mPXELdr int13h functions.
neoware
redefine computing.


Neoware Image Manager Boot Process
Comparison of boot process between an HD based client and a Neoware Image Manager client
HD based boot process
NTLDR is executed. Read and write requests emitted by NTLDR are processed by BIOS int13h functions. Boot.ini is processed. Boot drivers are loaded, among which the HD controller and disks drivers
The boot drivers, among which the HD controller drivers and disk drivers are initialized.
Neoware Image Manager based boot process
NTLDR is executed. Read and write requests emitted by NTLDR are processed by mPXELdr int13h functions. Boot.ini is processed. Boot drivers are loaded among which the NIC controller, TCP/IP, Neoware Image Manager client drivers and disks drivers
The boot drivers, among which NIC controller, TCP/IP, Neoware Image manager client drivers and disks drivers are initialized. Neoware Image Manager client drivers emit init requests to Neoware Image Manager server and customize the client, in particular its name.
If NeoDomain is installed, Image Manager kernel drivers read the domain credentials for the client currently booting and uses it as Windows Domain Credentials
neoware | redefine computing.


Neoware Image Manager Boot Process
Comparison of boot process between an HD based client and a Neoware Image Manager client
HD based boot process
Neoware Image Manager based boot process
The volumes accessible to the client are made available through standard Windows volumes drivers stack
The rest of the OS is loaded using the Windows Volumes drivers stack to access the data on the drives.
Shutdown time
If Client-Driven name change is enabled and the client name has changed, Image Manager kernel drivers sends to the server the new name for the client currently being shutdowned
If NeoDomain is installed and configured so that Domain Credentials are saved, Image Manager kernel drivers write the domain credentials for the client currently being shutdowned
neoware | redefine computing.

APPENDIX K

Troubleshooting

This appendix provides help on how to overcome problems when using Neoware Image Manager with various systems.

Technical Support

You can view our on-line support pages at the following Internet address:

http://www.neoware.com/support.php

Neoware offers various Technical Support programs. Check with your Neoware representative.

Check Versions

In case of a problem with Neoware Image Manager, especially if the product seems to work in some way (start booting but not finishing, boots completely but has “strange” behaviour), the first thing to do is to check that you are not mixing Neoware Image Manager components that come from different versions of Neoware Image Manager. In particular, `mPXELdr.bin`, `nvdd`, `BDruPD.SYS`, `NVD.SYS`, `DSKIMG.SYS`, `NDomMGR.sys` and `DomCred.sys` are made to work together and will not work correctly when used with components that come from another version of Neoware Image Manager.

In order to check versions, you can refer to the Release Notes document, or you can perform a “decompress” installation of Neoware Image Manager and check that the files you are using are actually the same as the ones in the “decompressed” folder.

File version information may be embedded in files made for Windows (`.EXE`, `.SYS`, `.DLL` etc.) or may be displayed on screen when they are run.

You can also refer to file dates and size, and you can use any file comparison tool.

PXE

PXE Implementations

Neoware Image Manager system works with all standard PXE 2.x compliant boot ROM code. Some PXE code implementations do not implement the complete PXE features.

So far, Neoware Image Manager has been used successfully with the following PXE codes:

- Intel Boot agent version 4.0.13 and after (Intel PRO/100 and PRO/1000 NICs).
- 3Com/Lanworks MBA version 4.00 and after.
- Realtek 8139 PXE (with Intel PXE Base code 082 and after).
- VIA Rhine II – VT6102/VT6103 (PXE NIC driver v2.07 and above).
- Broadcom NetXtreme Ethernet Boot Agent v 3.1.30 (also shipped as HP Boot Agent).
- Marvell Yukon PXE.
- SiS PXE.
- Bootix PXE Prom for Intel PRO/100 found in various Fujitsu/Siemens PCs.

If your adapter or PXE implementation is not listed here, it does not mean that it will not work with Neoware Image Manager.

In case it does not work as expected at the very beginning of the Windows 2K/XP boot process (e.g. you cannot see the first black and white character mode boot progress bar or Windows coloured splash screens, or the boot process is very slow), ask for an upgraded PXE code from the manufacturer of your NIC, motherboard or PXE code provider. The PXE implementation must correctly implement the complete set of UNDI functions. Some third party vendors provide PXE code for a large set of network cards.

Etherboot

Etherboot does not implement the complete set of PXE functions, so it cannot be used as the Pre-OS loading component to work with Image Manager. In particular, all the virtualization products that depend on Etherboot for their "PXE" (Xen and its variants - Virtual Iron, VirtualBox-, kvm...) will not be able to PXE-boot off Image Manager Server.

PXE Error File Not Found

This error is not actually related to Neoware Image Manager as it would also happen with any PXE related product. We provide this article for your information.

If you are using MS DHCP server on the server (and possibly other DHCP servers) and Intel Boot Agent v4.0.19 on the diskless client, please read the following.

Issues

Running Neoware Image Manager software while using Intel Boot Agent ver 4.0.19, the client aborts on downloading `mPXELdr.bin`. The error message is one of the following:

```
PXE-T01: File not found,
PXE-T02: Access violation,
PXE-E3B: TFTP Error - File not Found,
PXE-E3C: TFTP Error - Access violation
```

Cause

Certain types of DHCP servers, especially MS DHCP Server, may supply boot file names that are not terminated in a null character. Intel Architecture Labs PXE 2.1 addresses the null terminated boot file names, but fails to work correctly if the DHCP boot file size option is not present when using Intel Boot Agent 4.0.19.

Solution

This issue has been corrected in Intel Boot Agent 4.0.22. Update Intel Boot Agent to version 4.0.22 or above.

Customers using IBA 4.0.19 and running into this issue can also work around it by setting DHCP boot file size (DHCP option 13, DHCP tag 13) as a non-zero value (ideally the size of the boot file, but any value is usually working).

Network Adapters

VIA Rhine Family

If the client computers use VIA Rhine family network adapters (or a compatible network adapter), then the Network Adapter driver may need to be updated. VIA Rhine family drivers shipped with Windows 2000/XP are not always compatible with the Neoware Image Manager system. If an incompatible driver was used, the error could result in one of the following:

- you could see messages similar to the following on the server: `vol #-1062729016 doesn't exist`
- client freezing just as Windows coloured splash screen is displayed.
- client not being able to boot (Windows coloured splash screen displayed constantly).

Once the clients use the latest drivers (version 3.68.0.453 or later) for VIA Rhine Network Adapter, the problem should disappear.

Servers with Several Network Adapters

If the server response to the client is unexpectedly slow and the server has several network card adapters, the Neoware Image Manager server module should be configured so that it is using only one of the server assigned IP addresses. Use the parameter `address` in the `nvdd` configuration file or use the Neoware Image Manager Console (**Tools** > **Generic Options** > **Network**) to specify which NIC to use.

Servers with multiple NICs using a teamed virtual network adapter should work correctly as long as the `address` parameter is set to the IP address of the virtual adapter (teamed adapter).

You may, from time to time, see messages related to errors 10054 (connection reset by peer) and 10065 (no route to host) in the server log on multi-homed server. When these messages appear, the server can usually go on working correctly. If not, you should set the address parameter in the server configuration to a specific IP address instead of 0.0.0.0.

Volumes

Multi-Volume Windows 2000 Clients

When Neoware Image Manager Clients running MS Windows 2000 are booted with several Virtual Volumes, it may be necessary to scan for hardware changes in order for Windows 2000 to detect the extra volumes.

The procedure is as follows:

1. From the **Start** menu select **Settings** > **Control Panel** > **System** > **Hardware**.
2. Right-click on the computer name and select **Scan for Hardware Changes**.

   A new device (Neoware Image Manager Emulated Hard Drive) will be detected.
3. It may be necessary to provide the `dskimg.sys` driver to the new hardware wizard. `Dskimg.sys` is located in:

<Windows System Root>\SYSTEM32\DRIVERS
(usually C:\WINNT\SYSTEM32\DRIVERS
or C:\WINDOWS\SYSTEM32\DRIVERS).

ACPI

Stand By & Hibernation

Stand By and Hibernation are currently not supported on Windows systems that run with Neoware Image Manager. NVD.SYS driver version 1.0.0.5 and after implements a mechanism that prevents Stand By or Hibernation to occur in most cases. If the system emits a request to enter into Stand By or Hibernation mode, NVD.SYS will refuse the request and Windows will display a message stating that Neoware Image Manager emulated Disk Drive device prevented the system from entering into Stand By or Hibernation mode.

Shutdown & Reboot

NVD.SYS Shutdown Delay

In order for disk read and write requests to be processed in a short period of time after Neoware Image Manager virtual disk drivers have received shutdown notification, a parameter in NVD.SYS can be tuned.

This parameter is a registry value. By default, it has the value 3, which means that disks requests can be treated during 3 seconds after Neoware Image Manager virtual disks have received the system shutdown request to power off or re-start the Client.

This grace delay may be needed by some system components, especially some network card drivers.

You can tune this parameter according to experience. If some problems at shutdown occur, such as the client PC not being actually shutdown, with black screen or still with the mouse pointer being displayed, you can increase the shutdown_timeout parameter. A

value of 10 (10 seconds) is usually enough to let all the system component that still need to access the virtual disks. On the other hand, if the shutdown time seems too long, you can reduce this parameter value.

Please refer to the appendix "NVD.SYS Reference" on page 341 for more details about this parameter.

Windows 2000 Without the Latest Service Pack

When remote booting a Windows 2000 OS that has not had the latest service pack applied, the clients may not be able to shutdown or reboot, or may take up to half an hour to complete the reboot process. To solve this problem, apply the latest Windows 2000 service pack to the client OS. Windows service packs can be applied on virtual volumes when mounted in Admin mode (if there is enough free disk space on the client computer).

Startup

Clients Using Intel i810 Chipset Under Windows 2000

Clients using Intel i810 chipset under Windows 2000 may have problems at startup such as system freezing, blue screens or unexpected reboots.

Users are advised to update the Intel Display Driver to the latest version available on the Intel Support Web Site and to apply the latest Intel Inf Update utility to the HD-Based Windows installation before building the HD image with Neoware Image Manager ClientBuilder. This usually resolves the startup problems with Neoware Image Manager Clients based on i810 chipset and running Windows 2000.

Inaccessible Boot Device

If you get an `Inaccessible Boot Device (STOP:0x0000007B)` blue screen when starting a Neoware Image Manager client, you should investigate client network drivers issues.

This problem is usually related to Neoware Image Manager client drivers failing to initialize the Virtual HD properly in the Windows Plug'n'Play stack.

Boot Process Stuck

This problem is usually related to the Neoware Image Manager Client component not being able to communicate with the Neoware Image Manager server module. This can happen, for example, if the server module is not actually running or if client drivers are using NVD protocol v1 when the server module is using NVD protocol v2. Make sure that the `mPXELdr.BIN` file that your TFTP servers are sending out comes from the same software package as your NVDD server software.

This problem can also occur if the server is using a Gigabit Ethernet adapter connected to a Gigabit Ethernet switch and the clients are using 100MB/s Ethernet adapters. In order to correct this issue the user should enable flow control on each Ethernet adapter and on the switches as well (if available).

Global Performances

Single Client Running Slowly

Depending on hardware and drivers, it has been reported that sometimes, the server and client NICs have problems talking together at the speed rate required by Neoware Image Manager system, resulting in a lot of packets being lost.

To try to solve this problem you can decrease the maximum number of sectors that a Neoware Image Manager client can request to read or write in a single request. This is described in the next section.

Number of Sectors Per Read/Write Request

The maximum number of sectors per read or write request is set using an `NVD.SYS` client driver parameter. By default, the maximum number is 128. When reducing this parameter, the performances may get better.

This parameter is handled by the following registry value in the client registry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NVD\sector_per_request
```

This parameter is a DWORD and can have a value in the range 2 to 128.

If the client is acting slowly when remote booted, it is recommended that you try setting this parameter to 32. If this gives better result, try 64 afterwards, and keep tuning until you have worse results. Values under 32 are usually not better.

***Tip**: Test these setting changes within CVolwrite/Normal mode. Once you are happy with the setting, use Admin mode to make the final change.*

Refer to the appendix “NVD.SYS Reference” on page 341 for more information.

Network Facilities

Global Connectivity

Neoware Image Manager uses essentially UDP protocol on port 2184 (this port can be modified). It is therefore necessary that the corresponding packets are not filtered by the network devices that stand between Neoware Image Manager clients and servers. If you use manageable network devices, you must configure them so that Neoware Image Manager packets can be sent and received by all the Neoware Image Manager clients and servers fast enough.

Clients should be able to communicate with their server with at least 70Mb/s of theoretical baud rate. Use of uplinked switches is thus not recommended.

1000BT/100BT Ethernet Switches

It has been reported that with some Ethernet switches that have 1000BT (GigaEthernet) ports connected to the server NIC and 100BT Ethernet ports connected to the clients, the clients may act very slowly.

This problem usually comes from the buffers assigned to the 1000BT ports in the switch not being large enough and the switch cannot use flow control to stop the server NIC from emitting pack-

ets. This results in lots of packets sent by the server being overwritten before they are dispatched to the 100BT ports.

You should also enable flow control on the client and server NICs, and on the Ethernet switches if available.

Please also refer to the section "Number of Sectors Per Read/Write Request" on page 362 for information on reducing the number of sectors in a single Neoware Image Manager request.

Operations on Virtual Volumes

Delayed Write Failed or Disk Full Error in Client OS

The error `Delayed Write Failed` may be raised by Windows when write operations on virtual volumes were not able to complete successfully.

There are three major reasons for this error to appear:

- Not enough free space in the client partition where the write operations are to be performed.
  Resolution: Free some space in the client partition or build a larger HD image.
- Not enough free space in the server partition where the server-based write cache (CVol) files are stored.
  Resolution: Free or add some space in the server partition.
- The server-based write cache (CVol) file is filled to its maximum. The server then displays a corresponding error message in its logs.
  Resolution: Edit the current `nvdd` configuration file for Neoware Image Manager server and increase the parameter `sectors_map_size` (the default value or, if it exists, the value associated with the actual volume with the filled CVol file. Changing the maximum size of CVol data files just for the affected volume is the best solution). Restart the Neoware Image Manager server module or reload the configuration file. *Note that*

*you can also use the Neoware Image Manager Console to set this parameter (**Tools** > **Generic Options**, or the **CVol** tab in **Volume Properties**).*

Note that using any variant of CVolWrite mode with clients that are never restarted or that are up and running for long periods of time is very likely to lead to a "CVol file full" error. If you cannot restart your clients (for example, schedule an automatic reboot at night), you should then increase the CVol size, potentially up to the Image File size (but not above, as this would be useless).

There is also a minor reason for this error to occur:

- Not enough client licenses for Neoware Image Manager server. If the `Delayed Write Failed` error occurs and Neoware Image Manager server displays the message `Clients Count Exceeded` (in its log, Console messages or in Events Viewer), you need to obtain some more client licenses or to use fewer clients attached to your Neoware Image Manager server. You can also increase the parameter `max_idle_time` in the current `nvdd` configuration file so that connections between clients and server are not closed too early. Restart the Neoware Image Manager server module after having changed this parameter.

Delayed Write Failed Warnings

`Delayed write failed` warnings appear when a logical volume is filled up. Windows 2K/XP can use FAT, FAT32 and NTFS filesystems that are made so that, statistically, all the sectors will be written some day, even if the logical volume has more than 90% of free space.

In order for logical volumes not to get filled up too quickly, you can use CVolwrite/Volatile mode. The `nvdd` configuration file settings are:

```
<VolumeName>.write_mode=cvol_write
<VolumeName>.cvol_mode=volatile
```

The number of sectors written in a CVol file will then be only the ones that are written during a session (between reboots of the client).

This will also make sure the logical volume is always clean at boot time.

When CVolwrite/Volatile mode is not acceptable, you may schedule deletions of the CVol files on an acceptable basis (every night, every 3 days, every weekend etc…). A deletion batch file should:

1. CD to the directory where the CVol files are stored.
2. Shutdown all the clients that may have mounted a virtual drive off that server.
3. Stop the Neoware Image Manager server module.
4. Delete all the CVol files.
5. Re-start the Neoware Image Manager server module.

If your client OS is Windows XPe (Windows XP Embedded), you can enable Enhanced Write Cache. Then the clients will not actually write any data in the CVol data files.

To reduce the number of different sectors that are written during a user session, you should preferably use NTFS file system for the client volumes. If this is not possible, use FAT32 file systems and, as the last choice, use FAT file system.

Using compressed NTFS as the file system for the client volume is also a way to reduce the number of sectors that are written during a user session. To be efficient, the whole volume should be compressed. This compression should be done on the reference client hard disk, before Neoware Image Manager Client Builder is run.

To reduce the number of different sectors that are written during a user session, you should set the virtual memory of the clients to use a local hard disk, if any. If no local hard disks are present or available to store the Windows swap file, you should set the virtual memory size to a reasonable size. The minimum and maximum size for virtual memory should be set to the same values. The size of the virtual memory file (also known as a "page file" or "swap file") should not exceed the maximum number of sectors in a CVol file divided

by 8 (or the maximum CVol data size expressed in Kilobytes divided by 4).

For example, if the maximum number of sectors in a CVol is 1048576 (the maximum size of a CVol is then 512MB), the maximum size of Virtual Memory file should be 128MB.

To reduce the number of different sectors that are written during a user session, you should make sure that the auto-defragmentation feature in Windows XP is disabled (it is disabled by default by Neoware Image Manager Client Builder when it builds the HD image).

You can also set the maximum size of the CVol files to be the exact size of the image. In such a situation, it is possible that all the sectors originally present in the Image file are modified and are actually located in the CVol file. Note that having a lot of large CVols actually in use on a server will decrease performance. There is a simple reason for this. When several clients request a sector, there is a high probability that this sector is in fact in the Image file itself, and then the server reads it only once and keeps it in its disk cache. If each client uses its own copy of this sector, the server actually reads it several times (it actually reads several different sectors in each CVol data file) and will be unlikely to keep anything useful in its disk cache.

To reduce the number of different sectors that are written during a user session, you should make sure that the virtual volume is defragmented. This can be done before the virtual volume is created by Neoware Image Manager Client Builder, or afterwards, with the volume mounted in Admin mode.

Large File Support on Linux 2.2

Error When Opening a Large Volume

On some Linux servers you may encounter a `File Too Large` error when NVDD starts and tries to open a volume file that is larger than 2GB. This is caused by the lack of Large File Support in some Linux systems.

Without Large File Support, Linux cannot handle file sizes bigger than 2GB.

Resolution:

1. Make sure your Linux can handle files bigger than 2GB. If not, you may need to build a new kernel with Large File Support.
2. Make sure you use NVDD version 1.0.0.15 or later. All the versions of NVDD after 1.0.0.15 have complete Large File Support.

Computer SIDs

Neoware Image Manager clients that boot from the same HD image will all have the same machine SID. This is usually not a problem, especially when the clients are members of a domain and the local users accounts are not used to authenticate users. Yet, if having a different SID for each client is required, you can use Neoware Image Manager's Persistent Client Mode, or Normal Client Mode, in conjunction with any of the SID changer tools, for instance **NewSID**, from sysinternals, which you can find here:

```
http://www.microsoft.com/technet/sysinternals/Security/
NewSid.mspx
```

You can also use Microsoft's sysprep and even configure your image so that sysprep is run automatically to reseal the Windows installation the first time it boots a client (in CVolWrite/Normal mode). Then the changes will be done in the CVol space and will be kept until next time when the image is modified. At that time, the

CVol spaces will be discarded and your image should then run sysprep automatically.

It is recommended that you completely understand what the potential problems of duplicated SIDs could be before you configure Neoware Image Manager clients booting from the same disk image to have different SIDs. *Usually, there are absolutely no problems with Neoware Image Manager clients having duplicated SIDs, especially when the clients are member of a domain or when the mounting mode of the system Virtual HD is CVolwrite/Volatile.*

Refer to the following for more information regarding this matter:

`http://www.appdeploy.com/articles/sids.shtml`

`http://www.microsoft.com/technet/sysinternals/Security/NewSid.mspx`

Limitations

Data Transfer During Single Client Boot-up

Our measurements revealed that a single diskless Neoware Image Manager client that boots Windows XP using the default Neoware Image Manager configuration involves the transfer of approximately 80 MB of data on the LAN. Depending on each configuration, this amount of data may vary, usually between 60 MB and 100 MB.

Maximum Clients Attached to a Single Server

There is no theoretical limitation to the maximum number of clients that can be attached to a single Neoware Image Manager server. As long as there are enough bandwidth and hard disk resources on the server and network to serve all the client requests in an acceptable time (3 minutes to boot-up in the following example), you can use as many clients on a single server as required.

The following considerations are provided to help you design your Neoware Image Manager architecture properly. This section is merely theoretical and stands only as recommendation, nothing here is guaranteed.

A large number of stations on one single server *MAY* be supported, with no warranty, with a configuration in which the following recommendations are met:

1. The server should have at least 2 Ethernet 1000 NICs teamed as a single network adapter so that the server theoretical bandwidth is 2Gb/s or more.
2. The Ethernet switches should have 1000-100Mb/s capabilities and should be able to handle correctly large amounts of buffered packets, *WITHOUT DROPPING THEM.* (You may need to enable flow control on the switches and on the clients and server NICs.)
3. The Ethernet switches must NOT be uplinked. Stacked switches with a "back pane BUS" supporting at least 3GB/s may be used, so that each Ethernet port on which the clients are connected can have a large amount of private bandwidth.

   Each client should be able to get 100MB from the server in 3 minutes, even when all the clients are accessing the server at the same time.

   This means that for 150 clients, the needed theoretical bandwidth is:

   *100*1024*1024*8*150/(3*60) = 666.66 Mb/s*
4. The server should have several very fast local hard disks. The directory where the disk image is stored should be on one physical hard disk. The directory where CVol files are stored should be on one other physical hard disk. The server hard disk and HD controllers should have large buffers and cache.

   If your server has a RAID controller, it is recommended that you use RAID1 instead of RAID5.
5. The server should not be running ANY additional application that consumes CPU power, memory, disk access or network bandwidth.

6 The clients should have enough memory for the Page File (swap file) to be disabled or reduced to its minimum (around 20MB).

7 The clients should only run useful applications, not any Network/HardDisk consuming application such as video streaming, games... etc..

When designing a fleet of Neoware Image Manager stations, you should keep in mind that each client needs to have enough of the global bandwidth, and server disk access should be designed in consequence.

Such a project may require some field tests with the expected number of clients and server in order to design the system correctly.

Clients Booting Same Images on Several Servers

You can use Clustered servers, using any of the various Clustering systems available, for the OSes that can run Neoware Image Manager server module with a unique IP address assigned to the cluster of servers.

Maximum Number of Applications Run from an Image

The number of software applications that can be run at the same time on the same diskless client is related more to the client specification than to Neoware Image Manager. In particular it depends on client CPU power and client available memory. Neoware Image Manager has a side effect on memory because of the recommended limited virtual memory file (swap file). It depends also if the programs are using the virtual hard disk intensively or not. If they are using the virtual HD intensively, performances may decrease when a lot of programs and/or clients are using these programs at the same time.

Recommended Network Configuration

The following network configuration recommendations should help you to achieve better performances and avoid congestion.

- Never use uplinked Ethernet switches.
- Use good quality Ethernet controllers on the server and the clients.
- You can use teamed network adapters on the server to increase server network bandwidth.
- Use fast HDs on the server. The fastest the server HDs, the better performances.
- If your server disk controller is a RAID controller, it is recommended that you use RAID1 instead of RAID5.
- Use HDs with large internal disk cache (buffers) on the server.
- Use a large amount of RAM on the server and maximize disk caching on the server.
- Use good quality Ethernet switches that can be configured to support flow control and that have enough buffers to hold large amount of data between 1000BT and 100BT networks.
- Have enough RAM in the client (256MB or more).
- Limit the client virtual memory size or disable virtual memory on the clients.
- Use CVolwrite/Volatile mode for virtual HDs.
- Configure Windows on the client PCs to limit writes on the system drive (`C:`) as much as possible. A RamDisk can be useful for such purposes. Write Filters on Windows XP Embedded may be used.
- Limit the writes on Virtual HDs (use `My Documents` folder redirection, store the users e-mail folders on another server etc. and limit the user profiles sizes).

- If local Hard Drives are available to the clients, configure Windows so that its swap file is stored only on local HDs. Temporary folders can also be stored on local HDs.
- Check that each client will have enough network bandwidth to transfer data from and to each server.

APPENDIX L

Copyright Notices & License Terms

This appendix provides the copyright notices and license terms for software embedded in Neoware Image Manager components.

Patents

Neoware Image Manager software suite is protected by a number of patents: EP1808763, EP1728164, WO2007006960, WO0193016.

Patents pending.

Third Parties Copyrights

Neoware Image Manager embeds software codes that are copyrighted by third parties.

Here are the corresponding copyright notices and license terms.

Software Copyrighted by Aladdin Enterprises

Author: L. Peter Deutsch
E-mail: ghost@aladdin.com

Copyright (C) 1999, 2002 Aladdin Enterprises. All rights reserved.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Software Copyrighted by Paul Kocher

Author: Paul Kocher
E-mail: pck@netcom.com
Date: 1997

Software Copyrighted by Brian Gladman

Copyright (c) 1998, Dr Brian Gladman, Worcester, UK. All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. Distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. Distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. The copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

Software Copyrighted by Lukas Gebauer

Project: Delphree - Synapse 003.006.004

Content: **HTTP client**

Copyright (c)1999-2003, Lukas Gebauer. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Lukas Gebauer nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permison.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Initial Developer of the Original Code is Lukas Gebauer (Czech Republic).

Portions created by Lukas Gebauer are Copyright (c) 1999-2003.

All Rights Reserved.

Contributor(s): History: see HISTORY.HTM from distribution package (Found at URL: http://www.ararat.cz/synapse/)

Project: Delphree - Synapse 002.002.003

Content: **SNTP client**

Copyright (c)1999-2003, Lukas Gebauer. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Lukas Gebauer nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permision.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS

OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Initial Developer of the Original Code is Lukas Gebauer (Czech Republic).

Portions created by Lukas Gebauer are Copyright (c)2000-2003. All Rights Reserved.

Patrick Chevalley

History: See HISTORY.HTM from distribution package (Found at URL: http://www.ararat.cz/synapse/).

Software Copyrighted by Jordan Russell

Copyright (C) 1997-2003 Jordan Russell. All rights reserved.

This software is provided "as-is," without any express or implied warranty. In no event shall the author be held liable for any damages arising from the use of this software.

http://www.jrsoftware.org/

Index

A
access
  client images 59
ACPI
  considerations 115
  troubleshooting 360
activating Windows products 118, 127
Active Cloner 271
  clone directly to attached HD 273
  clone to another Image Manager virtual HD 275
  clone to network shared HD 274
  command line options 277
  error messages 279
  Expert options 276
  NimCloner.exe 277
  NimClonerGUI.exe 272
  restore volume to actual HD 144
adding
  network boot device to an image 87
  new application 83
  new client 11, 135
  new hardware 11
  new software 136
  new volume 70
  volume from another configuration file 209
Admin IP address 205, 217
Admin write mode 83, 136, 227
assigning volumes to clients 65
automatic updates
  disable 56

B
binaries
  directory for 219
boot process 9
bootable virtual drives 10
booting 68, 191, 235
  adding net boot device to image 87
  clients using same images on several servers 371
  mPXELdr.bin 59
  multiboot 68, 191, 235
  primary bootstrap loader file 59
  troubleshooting 360
  volume to boot from 191
buffer size 199, 223
building a client image 39
  testing 54
building a hard disk 103
  basic procedure 106

C
certificate file 202
certificate file for SSL 221
changing client name 234
ChkDsk 55
client

accessing images 59
activating Windows products 127
adding new 135
adding to Windows domain 147
assigning volumes to 65, 69
boot volume 68, 191, 235
changing name 234
configuring for images 62
display shared volumes 197
image
creation 39
testing 54
installation requirements 19
license file 16
local HD access 123
locating Image Manager server 317
MAC address 224
maximum attached to server 369
mPXELdr.bin 62
multiboot selection 68, 191, 235
naming 233
primary bootstrap loader file 62
renaming 348
server crash recovery 348
requirements 19
using Client Builder 40
volume use 79
writing modes 12
Client Builder 39
advanced options 55
executable file 40
introduction 39
NeowareIMClientBuilder.exe 40
running 40
undo changes 38
client files location 202
client volume overlay files 80
cloning
directly to attached HD 273
to another Image Manager virtual HD 275
to network shared HD 274
cloning current partition 271
command line options
Active Cloner 277
CVolCompactor 178
CVolMerge 178
nvdd 337
computer name change 222, 225
configuration file
adding volumes from another config file 73
allowed volume users 231
buffer size 223
copied to root file transfer folder 346
current 347
CVol file
location 218, 230
max size 221
description 213
editing 79
editing using Image Manager Console 181
example 238
group definitions 231
IP addresses 217
lock file 348
merging contents from another 209
modifying while running 75
nvdd 213
nvdd to read 338
nvdd.smalldisk.vol.conf 214
port number 217
processing units 223
server crash recovery 347
settings 217
temporary file 347
timing 218
user definitions 223
volume
cache size 230
definitions 225
geometry 226
ID 225
name 225
write mode 227
controlling use of volumes 79
copyright notices 375
creating
client image 39

introduction 39
using Client Builder 40
volume 193
current configuration file 347
CVol files
description 80
location 81, 196, 201, 218, 230
maximum size 81, 196, 199, 221
merging with image file 137, 177
reducing size before merging 177
size of 32
storage requirements 32
CVolCompactor 177
CVolMerge 137, 177
CVolwrite mode 83, 227

D

daylight saving 56
Defrag 57
detecting new hardware 110, 111
DHCP
disable Windows DHCP client 327
example dhcpd.conf file 318
how clients locate server 317
integrated DHCP client 327
options 319
reference 317
reservations 312
resources 315
server configuration 59, 297
Windows DHCP client 327
dhcpd.conf file 318
directory
for binaries 219
for file transfer 219
disable
autocheck on startup 55
automatic updates 56
ChkDsk 55
daylight saving 56
Defrag 57
memory dumps 57
system restore 58
disk storage required on server 32
domain
adding clients to 147, 159, 168, 174
client IP addresses 168
client names 159, 174
credentials 148
management 147
roaming profiles 131
storing credentials in server directory 151
storing credentials in system partition 170
storing credentials on non-volatile drive 162
user profiles 131
Domain Management wizard 147
drivers
updating for off-line devices 112

E

evaluation version 17
expiry date
UbiBoot 119

F

file location
CVol files 81, 196
Image Manager server 32
license file 33
nvdd server module 32
file transfer 345
directory for 219
root folder for files 345
file transfer files location 202

G

global performances 362
group definitions 231
group properties 191

H

HAL
multicore computers 115
selection 115
unicore computers 115
HAL considerations 113
hard disk
building 103

building procedure 106
cloning 271
for booting any PC 103
local client access 123
partition size 19
use unknown hardware 110
using when UbiBoot-enabled 110
hard drive
SATA 104
SCSI 104
hardware upgrade without re-installing software 113

I
IEEE 1394 interface (FireWire) 360
image
adding network boot device 87
Image Manager
evaluation version 17
how it works 8
installing 19
licenses 15
limitations 369
overview 7
uninstalling 35
upgrading 289
Image Manager components
Active Cloner 271
Client Builder 39
CVolCompactor 177
CVolMerge 137, 177
Domain Management wizard 147
Image Manager Console 181
Local HD Manager 123
LocalHDManager.exe 123
mPXELdr.bin 59
MS-TFTP Server Helper 294
NeoDomain.exe 147
NeowareIMClientBuilder.exe 40
NimCloner.exe 277
NimClonerGUI.exe 272
nvd.sys 341
nvdd server module 33, 40
nvdd.exe 33, 337
nvdd.smalldisk.vol.conf 214
NvddPasswd.exe 210
Service Loader Setup 329
smalldisk.vol 213
SrvcLoader.exe 329
SrvcLoaderSetup.exe 329
TFTPD Installer 293
TFTPDInstall.exe 293
UBExtract.exe 87
UbiBoot 103
UbiBoot Extractor 87
UbiBoot Inserter 87
UBInsert.exe 87
Image Manager Console 65
adding a new computer 67
adding a new group 68
assigning a volume to a group 69
certificates file 202
client files location 202
controlling image usage 79
controlling volume usage 79
creating a new volume 70
creating volumes 193
CVol files
location 201
maximum size 199
description 181
Edit menu 184
File menu 184
Generic Options 199
Authorized Subnets 206
Directories 201
General 199
Network 205
Help menu 186
Merge Information 209
Nvdd Manager 207
password for remote administration 210
properties of items 186
running 65, 181
toolbar 181, 183
Tools menu 185
View menu 186

Volume Properties
Allowed Computers 198
Computers 197
CVol 196
General 193
Parameters 195
Image Manager Service Loader Setup 329
images
accessing 59
adding new software 136
configuration file 65, 79
controlling use of 79
creating 39
CVol files 80
managing multiple remote servers 141
master HD for building 110
modifying configuration 136
nvdd configuration file 213
size 19
testing 54
troubleshooting 63
updating multiple remote servers 141
using Client Builder 40
installing Image Manager 19
InstallShield wizard 24
procedure 23
server configuration 32
system requirements 19
uninstalling 35
installing UbiBoot 104
InstallShield wizard 24
introduction
about this manual 2
adding new desktop 11
boot process 9
Client Builder 39
client writing modes 12
creating a client image 39
how Image Manager works 8
Image Manager components 7
Image Manager overview 7
server setup in organisation 8
UbiBoot 103
user manual overview 3
IP addresses 205, 217

L

lanpccltnn.lic 16
lanpcsrv.lic 16
license file 15
client package 16
example 16
location 33
server 16
license terms 375
load balancing 14
local HD access 123
Local HD Manager 123
local roaming profiles 132
LocalHDManager.exe 123
locating Image Manager server 317
lock file 348
log nvdd server activity 338

M

MAC address 224
master HD for building images 110
memory
dumps 57
virtual 57
merging
configuration files 209
image & CVol files 137, 177
Microsoft Sysprep 118
Microsoft VirtualPC 287
mPXELdr 59, 235
mPXELdr configuration file 251
contents & syntax 253
example 255
introduction 251
keywords 256
BootMode 260
Include 256
NICRxTxQs 268
NVDServers 258
PreBootPause 266
ReQueryDHCPOptions 267

VolSelectionTO 265
mPXELdr.bin 9, 59, 295, 311, 318, 320, 357
MS-TFTP Server Helper 294
multiboot selection 68, 191, 235
multicore computers 115
multi-CPU computers 115

N

NeoDomain.exe 147
Neoware Virtual Disk 9
Neoware Virtual Disk Daemon 9
NeowareIMClientBuilder.exe 40
NetBIOS name 326
network
  adapters 358
  adding boot device to an image 87
  configuring for image access 59
  installation requirements 19, 22
  recommended configuration 372
  requirements 22
  troubleshooting 358, 363
new hardware 111
  detecting 110
NimCloner.exe 144, 277
NimClonerGUI.exe 272
Normal CVolwrite mode 83, 228
NTLDR 10
NVD 9
NVD protocol 13
NVD.SYS 360
nvd.sys
  drive shutdown delay 360
  parameters 341
NVDAdmin
  file transfer 345
nvdd 9
nvdd configuration file 65, 79
  allowed volume users 231
  binary files
    location 219
  buffer size 223
  certificate file 221
  client naming 233
  computer name change 222, 225
  CVol file
    location 218, 230
    max size 221
  description 213
  editing using Image Manager Console 181
  example 238
  file transfer files
    location 219
  group definitions 231
  IP addresses 217
  MAC address 224
  nvdd.smalldisk.vol.conf 214
  port number 217
  processing units 223
  settings 217
  timing 218
  user definitions 223
  volume
    cache size 230
    definitions 225
    geometry 226
    ID 225
    name 225
    write mode 227
Nvdd Manager 207
nvdd server administration 241
nvdd server module
  command line options 337
  display messages 337
  lock file check 338
  log file 338
  port number 338
  read configuration file 338
  running 34, 40, 337
  running as a Windows service 329
  stopping 34
  verbose mode 337
nvdd service
  changing settings 333
  configuring 329
  installing 329
  starting & stopping 333
NVDD temporary files 347

nvdd.current.conf 346
nvdd.exe 33
nvdd.smalldisk.vol.conf 214
NVDDAdmin 242
  command examples 243
  command syntax 242
  commands 243
NvddPasswd.exe 210
NVDTFP 345

O

overview 345
  Image Manager 7
  software suite components 7
  user manual 3

P

partition cloning 271
partition size 19
password for remote NVDD server 210
performance of network 362
Persistent CVolwrite mode 84, 228
port number 205, 217
port number override 338
primary bootstrap loader file 59
processing units 223
product activation
  Windows 118
properties
  client 187
  group 191
  volumes 192
PXE 8, 62, 318, 356, 357

R

recommended network configuration 372
remote Image Manager server
  managing 141
  updating images 141
replacing server 13
restoredfiles directory
  configuration files 348
  user_rep files 349
roaming profiles
  domain 131
  folders redirection 134
  local 132

S

SATA hard drive support 104
save computer name change 222, 225
script
  updating image on remote servers 141
SCSI hard drive support 104
server
  cluster of 14
  DHCP 297
  DHCP configuration 59
  Image Manager
    configuration 32
    disk storage required 32
    file locations 32
    how clients find 317
    maximum attached clients 369
  installation requirements 19, 20
  license file 16
  list of to contact 14
  replacing 13
  requirements 20
  setup in organisation 8
  TFTP configuration 59
SIDs 368
size of partition 19
smalldisk.vol 213, 214
software
  activating Windows products 127
  adding to image 136
  third party 375
software suite components 7
SrvcLoader.exe 329
SrvcLoaderSetup.exe 329
SSL certificate file 202, 221
startup
  troubleshooting 361
storage requirements on server 32
Sysprep 118
system requirements

installation 19
system restore 58
system virtual volume
restoring to actual HD 144

T

technical support 355
temporary NVDD files 347
testing
client images 54
TFTP server configuration 59
TFTPD
managing 295
TFTPD Installer 293
TFTPDInstall.exe 293
third party software 375
timing 199, 218
troubleshooting 355
ACPI 360
booting 360
client accessing images 63
computer SIDs 368
global performances 362
IEEE 1394 interface (FireWire) 360
image access 63
NVDD server crash recovery 347
NVDD server temporary files 347
PXE 356
shutdown 360
startup 361
technical support 355
UbiBoot 119
volumes 359

U

UBExtract.exe 87
UbiBoot 103
ACPI considerations 115
additional uses 113
detecting new hardware 110, 111
expiry date 119
HAL considerations 113
installing 104
introduction 103
master HD for building images 110
running 106
troubleshooting 119
unknown hardware 110
updating drivers for off-line devices 112
using UbiBoot-enabled HD 110
UbiBoot Extractor 87
UbiBoot Inserter 87
UBInsert.exe 87
unicore computers 115
uninstalling Image Manager 35
unknown hardware
UbiBoot 110
upgrading
hardware 11
Image Manager 289
upgrading hardware without re-installing software 113
user definitions 223
user profiles 131
folders redirection 134
user_rep files 348

V

VIA Rhine network adapters 358
virtual memory settings 57
virtual volume
restoring to actual HD 144
virtualized environments 281
adding VM support to existing images 282
Microsoft VirtualPC 287
other 288
VMWare 281
VMWare environment 281
adding VM support to existing images 282
private networks 284
public & private networks 284
running Image Manager in a VM 284
streaming disk images 281
Volatile CVolwrite mode 84, 228
volume to boot from 68, 191, 235
volumes
access 198, 231
adding from another config file 73, 209

allowed clients 231
allowed users 198
assigning to clients 65, 69
boot from 191
cache size 230
changing write mode 75
creating 193
creating new 70
CVol files 80
defining 193, 225
directory for 193, 218, 230
display clients sharing 197
geometry 226
ID 195, 225
naming 193, 225
nvdd configuration file 213
properties 192, 193
restoring to actual HD 144
size of 194
smalldisk.vol 213, 214
storage 32
troubleshooting 359, 363, 364
use of 79
write mode 75, 195, 227
  Admin 83, 227
  CVolwrite 83, 228
  description 82, 227
  introduction 12
  Normal CVolwrite 83, 228
  Persistent CVolwrite 84, 228
  Volatile CVolwrite 84, 228

W

Windows
  domains
    adding clients to 147
  prefetcher 58
  product activation 118, 127
  user profiles 131
Windows service 329
write mode
  Admin 83, 227
  changing 75
  CVolwrite 83, 227
  description 82
  introduction 12
  Normal CVolwrite 83, 228
  nvdd configuration file 227
  Persistent CVolwrite 84, 228
  setting for volume 82
  specifying using console 195
  Volatile CVolwrite 84, 228